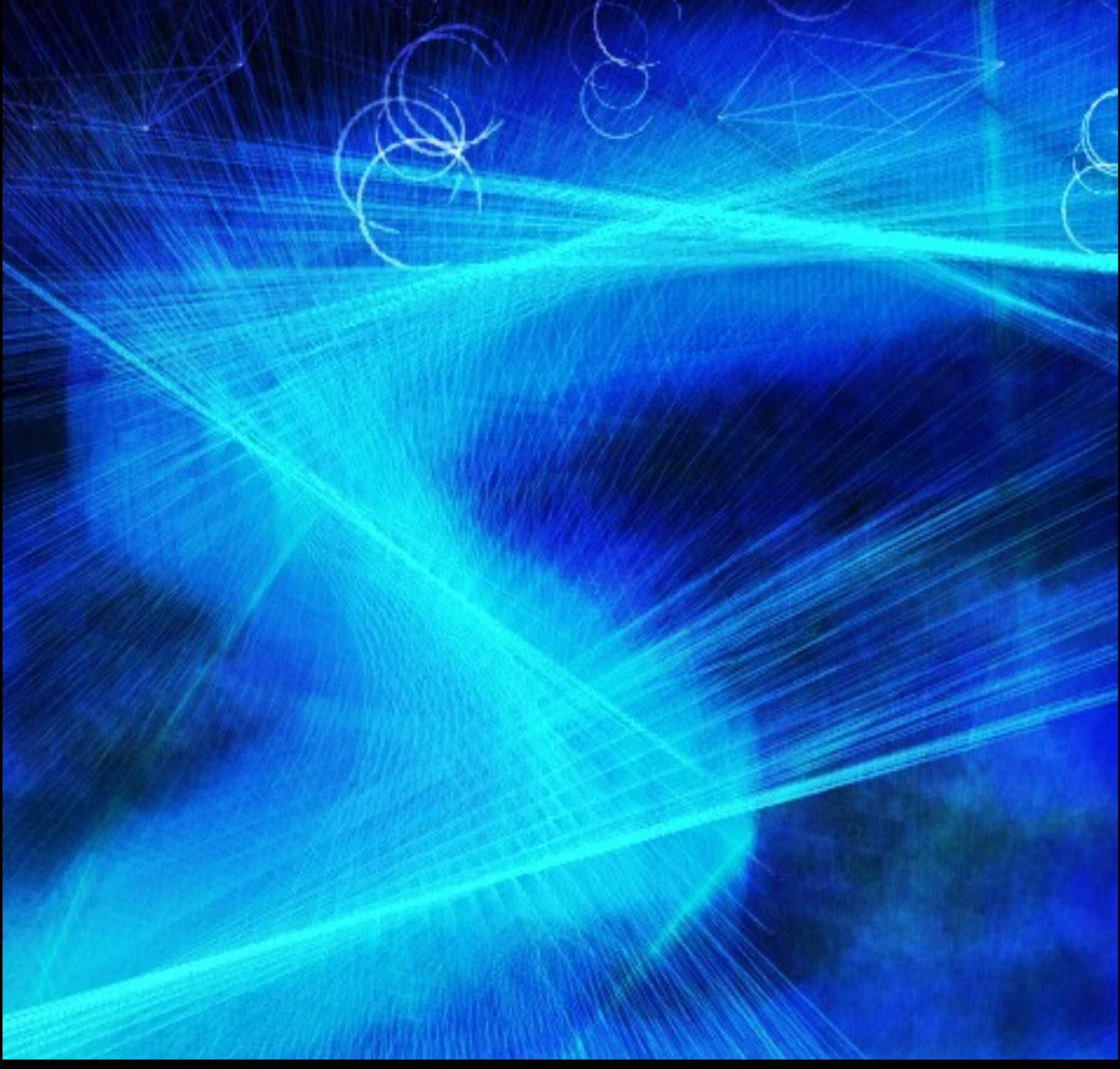
Higher School of Security and Economics, Plovdiv, Bulgaria

POLITICS & SECURITY

ISSN Print 2535-0358
ISSN Online 2815-3324



EDITORIAL BOARD

Founder and Publisher

Higher School of Security and Economics, Plovdiv, Bulgaria

ВУСИ

Journal Manager

E-SCIENCE SPACE, Warsaw, Poland

E-SCIENCE SPACE

POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

FOREWORD

Vol. 12 No. 2 (2025)

Dear Readers,

It is with great pleasure that we present the second issue of Politics & Security for the year 2025. This edition features a diverse selection of articles reflecting the interdisciplinary nature of our journal, encompassing critical topics at the intersection of security, economics, environmental sustainability, digital governance, and regional policy.

The issue opens with two empirical studies focused on occupational safety in Polish agriculture — a sector that continues to face structural and technological challenges despite its essential role in national food security. These articles offer not only a diagnostic view but also propose pathways toward enhanced legal and social frameworks for rural safety.

Expanding the scope internationally, we explore the impact of environmental and economic literacy on fish production in rural Bangladesh. This article is especially timely, as it underscores how local knowledge and resource management are pivotal for food and economic security in developing contexts.

The second half of the issue transitions toward broader geopolitical and security dynamics. From cyber sovereignty and energy security in the European Union to insider threats in governmental agencies, our contributors provide valuable perspectives on how states adapt to evolving risks. Of particular note is the article on security dynamics in the Black Sea region, which analyzes current tensions through the lens of NATO policy, Russian influence, and strategic economic interests — a topic of continuing global concern.

Finally, the inclusion of a forward-looking piece on climate change as a threat multiplier offers a sobering yet necessary reminder of the interconnectedness of environmental degradation, migration, and political instability. It is our hope that this issue will serve as a resource for scholars, practitioners, and policymakers alike.

I extend my sincere gratitude to all authors, reviewers, and members of the editorial team for their contributions. Your dedication ensures the continued growth and relevance of Politics & Security on the international academic stage.

Igor Britchenko

Editor-in-Chief

Politics & Security

CONTENTS

POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

ANALYSIS OF SAFETY AND CAUSES OF ACCIDENTS AT WORK IN AGRICULTURE IN POLAND

Janusz Kilar
Jan Grodek State University in Sanok
Sanok, Poland
jkilar@up-sanok.edu.pl
https://orcid.org/0000-0003-1886-2170

Małgorzata Szeliga
Jan Grodek State University in Sanok
Sanok, Poland
mszeliga@up-sanok.edu.pl
https://orcid.org/0009-0008-4967-8951

Magdalena Kilar
Regional Chamber of Audit in Rzeszow
Rzeszow, Poland
m.kilar@rzeszow.rio.gov.pl
https://orcid.org/0009-0000-6146-2039

Abstract: *The article analyzes the dynamics of accidents at work in agriculture in Poland in 2020–2021, taking into account factors influencing their occurrence and the effectiveness of preventive measures. Data comes from the Agricultural Social Insurance Fund, the Central Statistical Office and research by scientific institutes. It has been shown that the number of accidents decreased by over 50% in the period under review, but agriculture remains one of the most dangerous sectors of the economy. The main causes are technical defects of machines, lack of occupational health and safety training and work in inappropriate conditions. The conclusions indicate the need for further modernization of farms and intensification of training.*

Keywords: accidents, work in agriculture, prevention, work safety.

1. INTRODUCTION

Agriculture, as one of the basic branches of the national economy, plays a key role in ensuring food security, maintaining ecological balance and supporting sustainable development of rural areas. At the same time, it remains one of the most accident-prone sectors of professional activity, both in Poland and in other European Union member states. Accident statistics indicate that the number of incidents at work in agriculture remains at a relatively high level, despite technological progress, mechanization of field work and intensification of preventive measures carried out by institutions responsible for occupational safety (Pac, 2002; Pac, 2024a; Pac, 2024b). The characteristics of work in agriculture include a number of features that increase the risk of hazards: variability of weather conditions, physical intensity of work, multitasking, low saturation with safety procedures and frequent lack of technical and formal supervision. This situation is particularly visible in individual farms, which dominate the agrarian structure of Poland. In addition, work in agriculture is often performed by older people with a lower level of vocational education, which negatively affects compliance with occupational health and safety (OSH) rules. (Kowalski & Białkowska 2021; Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, 2023).

From a research perspective, it is important not only to capture the scale of the accident phenomenon, but also to identify its conditions, causal structure and socio-demographic determinants (Jędrasik-Jankowska, 2013; Jędrasik-Jankowska, 2003; Pac, 2006; Pac, 2018). A comprehensive analytical approach, combining empirical data with the assessment of organizational, technical and human factors, allows for a better understanding of the mechanisms leading to accident events and the formulation of effective prevention strategies. (Kordecka, 2008; Kordecka, 1997; Pac, 2022; Pac, 2023).

2. MATERIALS AND METHODS

The aim of the work is to conduct a multi-aspect analysis of the causes of accidents at work in the agricultural sector, taking into account the classification of risk factors, the characteristics of typical accident events and the presentation of statistical data illustrating the scale and dynamics of the phenomenon in 2020-2021. The analysis was based on available reports of the Central Statistical Office (GUS), the Agricultural Social Insurance Fund (KRUS) and scientific literature on work safety in agriculture in Poland.

The work includes a detailed analysis of data for 2020-2021 in the scope of:

- Structure of accidents by type of work performed;
- Structure of accidents by type of machinery and equipment;
- Causes of accidents by category (human, organizational, technical, other);
- Accidents by time of day;
- Accidents by day of the week;
- Accident rate and frequency of fatal accidents by voivodeship;
- Accident rate by province;
- Fatal accident rate by province.

3. RESULTS

The hazards occurring in the agricultural work environment are multifaceted and result from the impact of mechanical, biological, chemical and psychosocial factors (Matczak & Szpak 2022). The most frequently identified hazards include:

- Exposure to changing weather conditions – working in the open field implies the risk of overheating, hypothermia, dehydration and falls caused by reduced surface adhesion.
- Operating agricultural machinery and equipment – contact with moving parts of mechanisms is a significant source of injuries, especially in the context of improper technical condition or lack of protective covers.
- Hazards resulting from contact with farm animals – unpredictable behaviour of animals and errors in the organisation of work when handling them may result in bodily injuries of varying degrees of severity.
- Impact of chemical substances and biological factors – contact with mineral fertilizers, plant protection products, mycotoxins or organic aerosols increases the risk of poisoning, allergies and occupational diseases.

When analyzing the etiology of accidents in agriculture, the causal factors can be classified into four basic categories (Nowak, 2020; Kasa Rolniczego Ubezpieczenia Społecznego, 2023; Różański, 2023):

1. Technical factors:
   - deficiencies in the technical efficiency of machines and devices,
   - lack of mandatory protection of moving elements,
   - use of equipment not in accordance with its intended use or technical specification.
2. Organizational factors:
   - insufficient level of training in the field of occupational health and safety,
   - lack of operational procedures or their non-implementation,
   - improper planning and supervision of work processes.
3. Human (behavioral) factors:

– excessive physical and mental fatigue,
– reduced risk perception and routinization of professional behavior,
– undertaking work under the influence of psychoactive substances (alcohol, medicines, drugs).

4. Environmental factors:
– unfavorable microclimatic conditions,
– varied topography of the work area,
– insufficient lighting of workstations.

The elements defining an accident at work are: suddenness, external cause, injury or death of the employee and connection with work. Sudden event – an event characterized by the employee's surprise, something unpredictable, unexpected, sudden. External cause – a cause outside the employee's body. Injury – damage to body tissues or human organs. Work-related – occurs when there is a temporal, local and functional connection of a given event with work. An accident at work is considered to be an event (Świder & Piotrowski 2021): 1) sudden; 2) caused by an external cause; 3) resulting in injury or death; 4) which occurred in connection with work:

–during or in connection with the employee performing ordinary activities or orders from superiors;
–during or in connection with the employee performing activities for the employer, even without an order;
–while the employee was at the employer's disposal on the way between the employer's registered office and the place of performing the duty resulting from the employment relationship.

The analysis and characteristics of accidents at work in agricultural activities in Poland are conducted by the Agricultural Social Insurance Fund (KRUS). At the beginning of KRUS's operation, over 60,000 accidents were reported to organizational units annually (in 1993 - 66,000) (Kobielski, 2005). In recent years, a significant decrease in the number of accidents has been noted. In 2021, 12,000 were recorded. i.e. over 80% less, and the accident rate understood as the number of accidents ending with the payment of one-off compensations per 1,000 insured persons decreased in this period from 24.6 to 8.4.

This paper provides a detailed analysis of the structure of accidents over two years (2020-2021). During this period, 9,770 accidents were recorded in 2020 and 11,267 accidents in 2021, respectively. One of the main analyses that allow for the characterization of the accidents in question is the structure presented in terms of the type of work performed. A summary of data on the structure of accidents in 2020-2021 by type of work performed is presented in Table 1 below.

Table 1. Structure of accidents in 2020-2021 by type of work performed

Type of work performed	**Number of accidents**		**Share in %**		**2021-2020**	**2021/2020 in %**
	2020	**2021**	**2020**	**2021**		
Moving without load (to and from a location)	1 573	2 058	16.1%	18.3%	485	130.8%
Manual transport work - walking with carrying in hands, on shoulders, etc.	1 163	1 523	11.9%	13.5%	360	131.0%
Transport of loads using wheelbarrows, trolleys, etc.	137	116	1.4%	1.0%	-21	84.7%
Mechanical transport of animals, agricultural products and means of production	188	182	1.9%	1.6%	-6	96.8%
Work at heights (trees, stacks, piles, attics, lofts, scaffolding, etc.)	732	787	7.5%	7.0%	55	107.5%
Work in excavations, tanks and depressions	16	6	0.2%	0.1%	-10	37.5%
Cleaning work in the farmyard	226	312	2.3%	2.7%	86	138.1%
Agricultural work at home	74	86	0.8%	0.8%	12	116.2%
Maintenance, renovation, construction and demolition of buildings	353	318	3.6%	2.8%	-35	90.1%

Operation and use of agricultural machinery and equipment (including aggregation and adjustment, work in the field, orchard and meadow)	1 142	1 326	11.7%	11.7%	184	116.1%
Overhaul and repair of machinery and agricultural equipment	555	639	5.7%	5.7%	84	115.1%
Timber harvesting and processing (preparation of fuel, building material, etc.)	874	877	8.9%	7.8%	3	100.3%
Preparing pet food (steaming, grinding, etc.)	161	189	1.6%	1.7%	28	117.4%
Animal care (feeding, milking, zoohygienic treatments, driving away, etc.)	1 956	2 166	16.1%	1.7%	210	110.7%
Manual work on the farm, including the use of simple tools (rakes, hoes, forks, knives, secateurs, etc.)	269	294	16.1%	18.3%	25	109.3%
Processing of agricultural products (fruit, vegetables, meat, milk, cereals, etc.)	38	41	16.1%	18.3%	3	107.9%
Dealing with official matters, purchasing means of production, etc.)	49	53	16.1%	18.3%	4	108.2%
Other	264	294	16.1%	18.3%	30	111.4%
Total	**9 770**	**11 267**	**100,0%**	**100.0%**	**1 497**	**115.3%**

Source: Own study based on data from the Agricultural Social Insurance Fund

Analyzing the data in Table 1, it can be seen that most accidents occurred during work related to animal handling, e.g. feeding, milking, zoohygienic procedures, driving, etc. (1956 and 2166 accidents, i.e. 20.0% and 19.2%, respectively), moving around the farm without a load (1573 and 2058 accidents, i.e. 16.1% and 18.3%, respectively) and manual transport work (1163 and 1523 accidents, i.e. 11.9% and 13.5%, respectively).

When analyzing accident events in the analyzed period of 2020-2021, attention should also be paid to the size and structure of the number of accidents involving machines and devices used in agricultural activities (Table 2).

Table 2. Structure of accidents in 2020-2021 by type of machinery and equipment

	Number of accidents		**Share in %**		**2021-2020**	**2021/2020 in %**
Type of machines/devices	**2020**	**2021**	**2020**	**2021**		
Agricultural tractors	784	939	20.6%	22.2%	155	119.8%
Means of transport (passenger cars, motorcycles, bicycles, public transport, etc.)	131	148	3.4%	3.5%	17	113.0%
Means of transport (trailers, horse-drawn carts, delivery vans, etc.)	528	508	13.9%	12.0%	-20	96.2%
Cultivation machines and tools (harrows, ploughs, cultivators, etc.)	119	170	3.1%	4.0%	51	142.9%
Machines and equipment for sowing, planting, fertilizing and irrigation, including:	156	177	4.0%	4.2%	21	113.5%
grain seeders	32	34	0.8%	0.8%	2	106.3%
potato planters	17	24	0.4%	0.6%	7	141.2%
manure spreader	58	72	1.5%	1.7%	14	124.1%
fertilizer spreader	21	30	0.6%	0.7%	9	142.9%
other machines and devices for sowing, planting, fertilizing and irrigation	28	17	0.7%	0.4%	-11	60.7%
Machines and tools for plant care (for field, vegetable and fruit production, etc.)	70	77	1.8%	1.8%	7	110.0%
Machines and devices for plant protection (including dressing) and disinfection (e.g. sprayers, dressing machines, etc.)	52	50	1.4%	1.1%	-2	96.2%
Machines and equipment for harvesting crops, including:	302	361	7.9%	8.5%	59	119.5%

combine harvesters	116	131	3.1%	3.1%	15	112.9%
combines and other machines for root harvesting	55	78	1.4%	1.8%	23	141.8%
machines for harvesting hay, straw and green fodder	118	129	3.1%	3.0%	11	109.3%
other machines and equipment for harvesting crops	13	23	0.3%	0.5%	10	176.9%
Threshing machines and equipment, dryers and auxiliary equipment	15	37	0.4%	0.9%	22	246.7%
Machines and devices for cleaning and sorting crops and fruits	22	23	0.6%	0.5%	1	104.5%
Machines and equipment for feed processing (grinding machines, mixers, etc.)	67	79	1.8%	1.9%	12	117.9%
Machines and equipment for animal breeding and husbandry (for feeding, removing manure, caring for animals, etc.)	93	100	2.4%	2.4%	7	107.5%
Machines and equipment for timber harvesting and processing:	742	759	19.5%	17.9%	17	102.3%
circular saws	402	382	10.5%	9.0%	-20	95.0%
Chainsaws	235	259	6.2%	6.1%	24	110.2%
other equipment for obtaining and processing wood	105	118	2.8%	2.8%	13	112.4%
Other machines, devices and tools, including:	731	810	19.2%	19.1%	79	110.8%
hand power tools	265	298	7.0%	7.0%	33	112.5%
other machines, devices and tools	466	512	12.2%	12.1%	46	109.9%
Total	**3 812**	**4 238**	**100.0%**	**100.0%**	**426**	**111.2%**

Source: Own study based on data from the Agricultural Social Insurance Fund

Among all accident events recorded in the period under review, the high rate of accidents involving machinery and equipment used in agricultural activities is noteworthy. In 2020, the share of accidents in question was 39.0% (3,812 accidents) and in 2021 37.6% (4,238 accidents). Most of them occurred while operating agricultural tractors (20.6% and 22.2%, respectively), other machinery and equipment (19.2% and 19.1%, respectively) and various types of machinery for obtaining and processing wood (19.5% and 17.9%, respectively). With the participation of machinery and equipment, the most common events were from the following groups:

- ✓ catching, hitting by moving parts of machinery and equipment - 1,398 accidents, constituting 32.7% of all accidents involving agricultural machinery and equipment;
- ✓ falling of persons - 1,187 accidents, i.e. 27.8%; - other events (other events causing damage to health) – 531, i.e. 14.1%.

Available KRUS publications and studies on accidents in agricultural activities in the period under review also allow for characterizing the causes of accidents. The causes of accidents in 2020-2021 by category are presented in Table 3.

Table 3. Causes of accidents in 2020-2021 by category

	Number of accidents		**Participation (%)**		**2021-2020**	**2021/2020 (%)**
Category of causes	**2020**	**2021**	**2020**	**2021**		
Human:	**5 653**	**6 346**	**57.9%**	**56.3%**	**693**	**112.3%**
– improper conduct of the farmer	1 993	2 301	20.4%	20.4%	308	115.5%
– improper use of machines, devices and tools	1 220	1 441	12.5%	12.8%	221	118.1%
– the psychophysical condition of the farmer, which does not ensure safe performance of work	467	576	4.8%	5.1%	109	123.3%
– failure to use work safety and security devices	1 217	1 340	12.5%	11.9%	123	110.1%
– inappropriate behavior of the farmer	756	688	7.7%	6.1%	-68	91.0%
Organizational	**1 031**	**1 046**	**10.6%**	**9.3%**	**15**	**101.5%**

Technical:	**2 317**	**3 016**	**23,7%**	**26,8%**	**699**	**130,2%**
– improper condition of machines, devices and tools	356	394	3.6%	3.5%	38	110.7%
– improper condition of building structures	385	463	3.9%	4.1%	78	120.3%
– improper condition of the yard, communication routes, maneuvering areas, etc. on the farm	1 213	1 790	12.4%	15.9%	577	147.6%
– improper technical condition of ladders, platforms, scaffolding and other auxiliary equipment used on the farm	265	250	2.7%	2.2%	-15	94.3%
– improper condition of communication routes (roads, pavements, etc.) and construction facilities outside the farm	70	94	0.7%	0.8%	24	134.3%
– other technical irregularities	28	25	0.4%	0.3%	-3	89.3%
Other causes	**769**	**859**	**7.8%**	**7.6%**	**90**	**111.7%**
Total	**9 770**	**11 267**	**100.0%**	**100.0%**	**1 497**	**115.3%**

Source: Own study based on data from the Agricultural Social Insurance Fund

- The majority of accidents were caused by human causes – (5653 and 6346, respectively, i.e. 57.9% and 56.3% of all accidents analyzed in the reporting period. The largest share among them is occupied by:
- improper conduct of the farmer (1993 and 2301 accidents, respectively, i.e. 20.4% and 20.4%)
- improper use of machines, devices and tools (1220 and 1441 accidents, respectively, i.e. 12.5% and 12.8%)
- failure to use work protection and safety devices (1217 and 1340 accidents, respectively, i.e. 12.5% and 11.9%)

Separating from the above data technical causes (2317 and 3016 accidents, respectively, i.e. 23.7% and 26.8%), the largest share is occupied by:

- improper condition of the yard, communication routes, maneuvering areas, etc. (1,213 and 1,790 accidents, i.e. 12.4% and 15.9%, respectively);
- improper condition of buildings (385 and 463 accidents, i.e. 3.9% and 4.1%, respectively);
- improper condition of machines, devices and tools (356 and 394 accidents, i.e. 3.6% and 3.5%, respectively).

An additional, noteworthy factor in the structure of accidents conducted by KRUS is the breakdown of accidents by time of day and day of the week. Table 4 presents the number of accidents by time of day in 2020-2021.

Table 4. Accidents by time of day in 2020 - 2021

Time of day	Number of accidents		Share in %	
	2020	**2021**	**2020**	**2021**
in the morning (06:01 to 12:00)	3 492	4 027	35.7%	35.7%
in the afternoon (12:01 to 18:00)	4 864	5 546	49.8%	49.2%
evening (18:01 to 24:00)	1 191	1 417	12.2%	12.6%
at night (00:01 to 06:00)	223	277	2.3%	2.5%
Total	**9 770**	**11 267**	**100.0%**	**100.0%**

Source: Own study based on data from the Agricultural Social Insurance Fund

Below is a summary of the number of accidents on farms by day of the week in 2020-2021 (Table 5).

Table 5. Accidents by day of the week in 2020-2021

Day of the week	Number of accidents		Share in %	
	2020	**2021**	**2020**	**2021**
Monday	1 634	1 853	16.7%	16.4%
Tuesday	1 380	1 605	14.1%	14.2%
Wednesday	1 414	1 676	14.5%	14.9%

Thursday	1 426	1 664	14.6%	14.8%
Friday	1 489	1 678	15.2%	14.9%
Saturday	1 650	1 867	16.9%	16.6%
Sunday	777	924	8.0%	8.2%
Total	**9 770**	**11 267**	**100.0%**	**100.0%**

Source: Own study based on data from the Agricultural Social Insurance Fund

Data analysis allows us to draw attention to the days that stand out in terms of the increased number of accidents - Monday (16.7% and 16.4%, respectively) and Saturday (16.9% and 16.6%, respectively). The majority of accidents are recorded in the morning and afternoon (from 6:01 to 18:00).

For many years, the Agricultural Social Insurance Fund has observed a large variation in the accident rate between individual provinces. Data on the accident rate and data on the frequency of fatal accidents in 2021, divided by province, are presented in Table 6.

Table 6. Accident rate and frequency of fatal accidents in 2021 by voivodeship

Voivodeship	**Accident rate**	**Fatal accident rate**
	2021	
dolnośląskie	7.2	5.0
kujawsko-pomorskie	10.7	8.1
lubelskie	9.2	3.4
lubuskie	6.8	0.0
łódzkie	8.7	2.2
małopolskie	5.9	2.2
mazowieckie	8.3	4.2
opolskie	4.8	0.0
podkarpackie	7.7	1.2
podlaskie	10.8	6.2
pomorskie	8.6	13.1
śląskie	4.8	0.0
świętokrzyskie	7.8	31
warmińsko-mazurskie	9.4	2.5
wielkopolskie	10.2	6.3
zachodniopomorskie	5.7	0.0

Source: Own study based on data from the Agricultural Social Insurance Fund

The highest accident rate was recorded in the following provinces: Podlaskie (10.8), Kujawsko-Pomorskie (10.7), Wielkopolskie (10.2) and Warmińsko-Mazurskie (9.4), and the lowest in the Opolskie and Śląskie provinces (4.8). The large variation in the accident rate between provinces results from, among others, the profile of agricultural production, differences in terrain, disproportions in their infrastructure, as well as from the different economic situation of farms. Chart no. 1 presents the accident rate in 2021 divided by province.

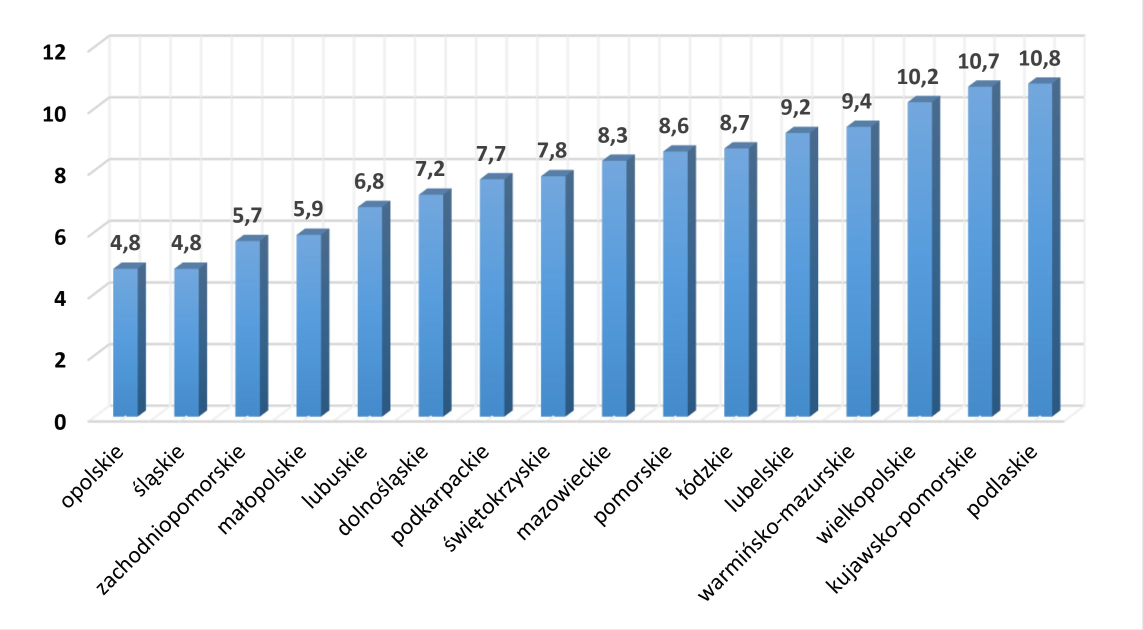


Figure 1. Accident rate in 2021 by province

Source: Own study based on data from the Agricultural Social Insurance Fund

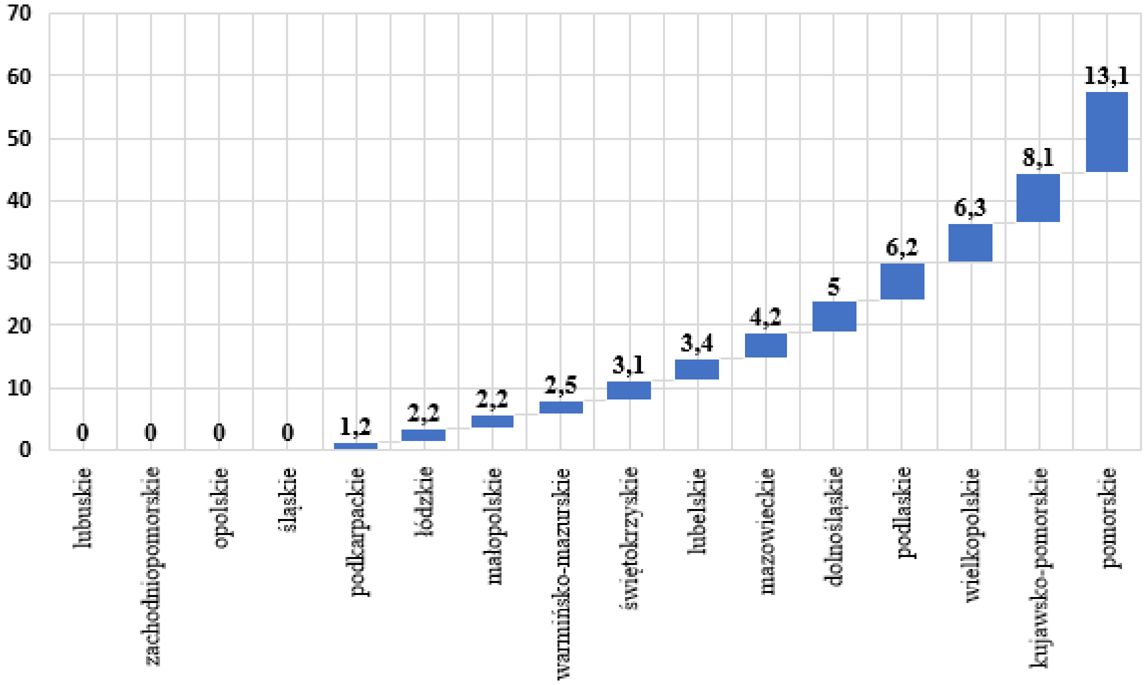


Figure 2. Fatal accident rate in 2021 by province

Source: Own study based on data from the Agricultural Social Insurance Fund

Fatal accidents accounted for 0.5% of all accidents resulting in the payment of benefits in 2021. Their frequency was 4 per 100,000 insured persons. The highest frequency of fatal accidents was recorded in the Pomeranian Voivodeship (13.1) and Kuyavian-Pomeranian Voivodeship (8.1), and the lowest in the Podkarpackie Voivodeship (1.2). On the other hand, no fatal accidents were recorded in the West Pomeranian, Silesian, Opole and Lubuskie Voivodeships in 2021. Data on the accident frequency rate are presented in Chart 2.

4. CONCLUSIONS

Among all recorded accidents, there is a high rate of accidents involving machinery and equipment used in agricultural activities. Most of them occurred while operating agricultural tractors, other machinery and equipment, and various types of machinery for obtaining and processing wood.

Most accidents occur due to human causes. The most common human errors include:

- ✓ improper conduct of the farmer,
- ✓ improper use of machinery, equipment and tools,
- ✓ failure to use protective clothing at work and safety devices.

However, technical causes should also be taken into account, in which the highest share is held by:

- ✓ improper condition of the yard, communication routes, maneuvering areas, etc.,
- ✓ improper condition of building structures,
- ✓ improper condition of machinery, equipment and tools.

Data analysis allows us to draw attention to the days that stand out in terms of the increased number of accidents - Monday and Saturday. It is probable that the increased number of accidents on Mondays is related to the farmer's Sunday rest.

In trying to develop and implement preventive principles for preventing accidents on farms, based on these studies, the most reasonable would be to first train farmers and workers working on farms in the principles of safe use of machinery and equipment, the need to use work protection and safety devices, as well as maintaining the infrastructure on the farm in proper condition. This would limit the negative social effects of such accidents, which in particular include:

- ✓ death as a result of injuries suffered,
- ✓ permanent damage to health (disability) that makes it difficult or impossible to run a farm,
- ✓ temporary inability to run a farm,
- ✓ increased public expenditure on health services,
- ✓ increased expenditure and pension and disability contributions,
- ✓ an increase in the number of people with a disability certificate.

Increasing expenditure on education and preventive measures, their effective development and implementation of the developed solutions would be an economically and socially beneficial action for both the Podkarpackie Province and the entire country.

The constant need to incur labor costs translated into the number of accidents recorded in agricultural activities in the province. Accidents on farms registered by the Agricultural Social Insurance Fund in Poland amounted to: 9,770 accidents in 2020 (2020) and 11,267 accidents (2021), respectively. Analyzing the data in terms of the type of work performed, it can be seen that most accidents occur during work related to animal handling, e.g. feeding, milking, zoohygienic procedures, driving, etc., as well as moving around the farm without a load and manual transport work.

REFERENCES

Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy. (2023). *Bezpieczeństwo pracy w rolnictwie – raport roczny 2022*. CIOP-PIB. https://www.ciop.pl

Jędrasik-Jankowska, I. (2003). *Ubezpieczenie społeczne, t. III: Ubezpieczenie chorobowe. Ubezpieczenie wypadkowe* (p. 148). Warszawa.

Jędrasik-Jankowska, I. (2013). *Pojęcia i konstrukcje ubezpieczenia społecznego* (p. 421). Warszawa.

Kasa Rolniczego Ubezpieczenia Społecznego. (2023). *Analiza przyczyn i okoliczności wypadków przy pracy rolniczej za rok 2022*. KRUS. https://www.krus.gov.pl

Kobielski, W. (2005). Wypadki przy pracy i choroby zawodowe rolników – wybrane problemy. *Ubezpieczenia w Rolnictwie. Studia i Materiały*, (2), 30.

Koradecka, D. (Ed.). (1997). *Bezpieczeństwo pracy i ergonomia* (p. 37). Centralny Instytut Ochrony Pracy – PIB.

Koradecka, D. (Ed.). (2008). *Bezpieczeństwo i higiena pracy* (p. 56). Centralny Instytut Ochrony Pracy – PIB.

Kowalski, R., & Białkowska, M. (2021). Zagrożenia zawodowe w gospodarstwach rolnych – analiza przypadków i kierunki prewencji. *Bezpieczeństwo Pracy: Nauka i Praktyka, 5*(598), 12–18.

Matczak, M., & Szpak, A. (2022). Przeciwdziałanie wypadkom przy pracy w rolnictwie – aspekty organizacyjne i techniczne. *Problemy Inżynierii Rolniczej, 30*(2), 25–35. https://doi.org/10.15576/PIR.2022.2.25

Nowak, T. (2020). Determinanty wypadkowości w rolnictwie indywidualnym w Polsce. *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, (3), 67–81. https://doi.org/10.15678/ZNUEK.2020.3

Pac, W. (2006). Dynamika przeobrażeń samorządowych w aspekcie kreowania podmiotowości jednostek i grup społecznych. *Seminare. Poszukiwania Naukowe, 23*(1), 195–212.

Pac, W. (2018). Służby specjalne w sferze bezpieczeństwa państwa. In *Człowiek – społeczeństwo – bezpieczeństwo* (pp. 42–58). Państwowa Wyższa Szkoła Wschodnioeuropejska w Przemyślu.

Pac, W. (2022). Prawne i instytucjonalne uwarunkowania ścigania przestępstw przerzutu imigrantów przez wschodnią granicę Rzeczypospolitej Polskiej jako zewnętrzną granicę Unii Europejskiej. *Przegląd Policyjny, 147*(3), 224–239.

Pac, W. (2023). Legal and institutional conditions for prosecuting smuggling of immigrants across the eastern border of the Republic of Poland as an external border of the European Union. *Przegląd Policyjny, 147*, 224–239.

Pac, W. (2024a). Demographic and social consequences of the Russo-Ukrainian war for Ukraine. *Politics & Security, 9*(3), 53–67.

Pac, W. (2024b). Humanitarian assistance for war refugees from Ukraine: A case study of the Podkarpacki Branch of the Polish Red Cross. *Politics & Security, 9*(3), 36–52.

Pac, W. (2025). Challenges and strategies in Poland’s policy towards Ukraine in the context of migration. *Politics & Security, 11*(1), 42–54.

Różański, A. (2023). Starzenie się ludności wiejskiej jako czynnik ryzyka w zakresie bezpieczeństwa pracy. *Studia Obszarów Wiejskich, 61*, 101–116. https://doi.org/10.7163/SOW.61.6

Świder, M., & Piotrowski, J. (2021). Czynniki wpływające na ryzyko zawodowe w sektorze rolnym w Polsce. *Journal of Agribusiness and Rural Development, 61*(3), 201–208. https://doi.org/10.17306/J.JARD.2021.01479

.

POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

WORK SAFETY ON FARMS IN POLAND – LEGAL, SOCIAL AND TECHNOLOGICAL CONDITIONS

Janusz Kilar
Jan Grodek State University in Sanok
Sanok, Poland
jkilar@up-sanok.edu.pl
https://orcid.org/0000-0003-1886-2170

Małgorzata Szeliga
Jan Grodek State University in Sanok
Sanok, Poland
mszeliga@up-sanok.edu.pl
https://orcid.org/0009-0008-4967-8951

Magdalena Kilar
Regional Chamber of Audit in Rzeszow
Rzeszow, Poland
m.kilar@rzeszow.rio.gov.pl
https://orcid.org/0009-0000-6146-2039

Abstract. *Agriculture is an economic sector with a high accident rate. Working on a farm requires acquiring knowledge, skills and experience in various fields. The specificity of this industry leads to many health and life hazards and a high risk of accidents. Farmers work in different positions, depending on what is produced on the farm. They operate machinery and equipment, as well as perform maintenance and repairs, participate in transport and storage processes, take care of farm animals, perform agricultural technical and chemical treatments and other non-agricultural activities. The simultaneous occurrence of many production and logistics processes increases the risk of accidents and makes work in agriculture more difficult. Transport and storage processes are common on farms. They are defined as a carefully organized system of interconnected logistics processes, the purpose of which is to produce agricultural products using land, labor, capital, management decisions (farmers) and the forces of nature. Statistics show that the most dangerous events can be considered those that occur during transport work and those related to the operation of tractors and agricultural machinery.*

Keywords: work safety, accident at work, farming, accident prevention.

1. INTRODUCTION

The working environment of farmers is very specific compared to other professions. The variety of work that farmers have to perform exposes them to many dangerous and harmful elements. Working hours are also irregular, often exceeding eight hours a day. Stress and rush have also contributed to the increase in agricultural accidents. The number of accidents has been high for many years and is not characterized by a decreasing trend. It is not possible to talk about only one cause, although inspectors investigating accidents usually point to one - the main cause. However, accidents occur for many overlapping reasons. Generally, the causes of serious accidents in agriculture should be sought in very complex agricultural work environments, where due to the work performed and the number of machines, tools, buildings used, contact with animals and variable conditions. Of the many threats, the greatest seems to be the lack of awareness among farmers. There are also historical reasons for this lack of awareness. For many years, farmers did not have any system of labor protection. As a result, they do not have the opportunity to participate in training, the aim of which is, among others, to building awareness of hazards and creating a safe work culture (Bińczycka-Majewska, 1993). It should be remembered that a farm is not only a place of work. It is also a living quarters for entire peasant families – often multi-generational – from working children to middle-aged and young people who simply play, as well as older people who feel the need to work among them, because they should not waste their energy. Another cause of agricultural accidents is the technical condition of equipment and buildings. The lack of possibilities to improve the situation due to the low level of farmers' income is another reason for the threat to the work environment in agriculture. About 70-80% of accidents are caused by human errors caused by the mentality of farmers, inappropriate behaviour at work or improper performance, passed down from generation to generation (Jaworska-Spicak, 2001).

2. MATERIALS AND METHODS

The aim of the work was to present Polish legal regulations concerning work in agriculture and the structure of accidents. This aim was achieved based on a query of national literature and analysis of existing data. It presents definitions of agriculture and accidents in agriculture. The importance and role of the Agricultural Social Insurance Fund is presented. In addition, the hazards occurring during agricultural work are discussed. Mechanical, chemical, biological and physical hazards are illustrated. The work also discusses the subject of accidents and the nature of occupational diseases in agriculture. The directions and forms of KRUS preventive actions at national and local level are discussed in the further part.

3. LEGAL REGULATIONS ON OCCUPATIONAL HEALTH AND SAFETY IN AGRICULTURE

Detailed legal regulations regarding occupational health and safety in agriculture are regulated in Poland by several acts and departmental regulations. These are:

- Act of 27 April 2001 - Environmental Protection Law. Announcement of the Speaker of the Sejm of the Republic of Poland of 23 January 2008 on the announcement of the uniform text of the act - Environmental Protection Law (Journal of Laws 2008, No. 25, item 150, as amended),
- Act of 13 April 2007 on the State Labour Inspectorate (Journal of Laws 2007, No. 89, item 589, as amended),
- Act of 25 August 2006 on food and nutrition safety (Journal of Laws 2006, No. 171, item 1225, as amended),
- Act of 14 March 1985 on the State Sanitary Inspectorate. Announcement of the Minister of Health of 4 May 2006 on the announcement of the uniform text of the act on the State Sanitary Inspectorate (Journal of Laws 2006 No. 122, item 851, as amended),
- Act of 26 June 1974 - the Labor Code (Journal of Laws 1998, No. 21, item 94, as amended),
- Act of 24 August 1991 on fire protection. Announcement of the Marshal of the Sejm of the Republic of Poland of 15 October 2009 on the announcement of the uniform text of the act on fire protection (Journal of Laws 2009, No. 178, item 138),
- Act of 11 January 2001 on chemical substances and preparations Announcement of the Marshal of the Sejm of the Republic of Poland of 27 August 2009 on the announcement of the uniform text of the act on chemical substances and preparations (Journal of Laws 2009, No. 152, item 122),
- Act of 20 December 1990 on social insurance for farmers. Announcement of the Marshal of the Sejm of the Republic of Poland of 10 March 2008 on the announcement of the uniform text of the act on social insurance for farmers (Journal of Laws 2008, No. 50, item 291, as amended),
- Act of 27 April 2001 - Environmental Protection Law. Announcement of the Marshal of the Sejm of the Republic of Poland of 23 January 2008 on the announcement of the uniform text of the act - Environmental Protection Law (Journal of Laws 2008, No. 25, item 150, as amended),

- Act of 13 April 2007 on the State Labour Inspectorate (Journal of Laws 2007, No. 89, item 589, as amended),
- Act of 25 August 2006 on food and nutrition safety (Journal of Laws 2006, No. 171, item 1225, as amended)

Direct enforcement is based on ministerial regulations, such as:

- Regulation of the Minister of Labour and Social Policy of 26 September 1997 on general occupational health and safety regulations (Journal of Laws 2003, No. 169, item 1650, as amended),
- Regulation of the Minister of Health of 30 December 2004 on occupational health and safety related to the presence of chemical factors in the workplace (Journal of Laws 2005, No. 11, item 86, as amended),
- Regulation of the Minister of Agriculture and Rural Development of 9 September 2004 on the qualifications of persons authorized to perform professional slaughter and the conditions and methods of slaughter and killing animals (Journal of Laws 2004, No. 205, item 2102, as amended),
- Regulation of the Minister of Social Policy of 28 April 2005 on the method and procedure for reporting an accident at agricultural work and determining its circumstances and causes (Journal of Laws 2005, No. 76, item 669),
- Regulation of the Minister of Health of 22 April 2005 on biological factors harmful to health in the work environment and the protection of the health of employees professionally exposed to these factors (Journal of Laws 2005, No. 81, item 716, as amended).

In Poland, the Agricultural Social Insurance Fund has been legally obliged to promote safe work of farmers, by the Act on social insurance of farmers of 20 December 1990 (Journal of Laws No. 7, 1998, item 25, as amended). Basically, in agricultural practice, due to the nature of work, it is impossible to completely eliminate harmful and burdensome factors, which is why society should be made aware of their existence in agriculture and their negative impact on the human body should be indicated (Pac, 2006).

An important educational element is broad activity promoting appropriate solutions and work methods. Popularization of occupational health and safety issues is of particular importance for raising the level of work culture. This is a long-term task with difficult to measure effects, but necessary for improving the state of occupational safety in agriculture. When speaking about work protection, we should take into account, to the extent available, all legal norms and observations, both our own and research, in the field of biological and technical processes occurring in agriculture, aimed at protecting the rights of an individual producer, employee, protecting their life, health and securing them against dangerous, harmful and burdensome factors for the body occurring in a given work environment (Pac, 2018). The definition of work protection also includes the concept of physical safety and biological hazards at work. In general, work safety should therefore be considered as activities aimed at protecting an employee, producer, farmer, breeder against accident hazards, i.e. those that ultimately contribute to the occurrence of an injury caused by an external factor, including biological, physical or chemical factors occurring in the work process. The essence of occupational health and safety is, above all, safe work organization while observing safe and rational human behavior in a given environment (Pac, 2023; Pac 2022; Wyka, 2001).

The labor protection system in Poland should primarily take into account:

- state supervision over working conditions,
- social supervision over health and safety conditions,
- liability for violation of labor protection regulations by employers and employees,
- rational and safe undertakings for the protection of labor on family farms (Miłkowski et al. 2014).

The main postulate of employees has always been, is and will be the systematic reduction or elimination of hazards occurring in the work process, and this requires knowledge of specific principles, health and safety regulations, sufficient knowledge and practical skills, and an active and responsible attitude of employees. For this purpose, actions are taken to popularize labor protection issues through dissemination, promotion and teaching, enabling the acquisition of knowledge, skills and adaptation to appropriate habits among wide circles of society, which should be implemented and included in the basic principles of health and life protection on a farm (Cież, 2013; Pac, 2025).

4. ACCIDENTS AT WORK IN AGRICULTURE

Despite the changes taking place in agriculture, the causes of accidents at work in agriculture have not changed over the years. The lack of ability to predict the effects of hazards by farmers plays a significant role here. The source of many accidents is carelessness, disregard for danger, haste, failure to use protective clothing and work footwear, poor technical condition of machines and devices used in agricultural production, ignorance of the principles of their safe operation. Among the listed causes of accidents, failure to comply with the principles of safe work still takes the leading place (Puślecki 2004; Pac, 2024a; Pac, 2024b). The concept of an accident is defined in the literature as "an unfortunate event, misfortune, catastrophe, a violent and unexpected phenomenon". An unfortunate event that happens to a farmer during work is sometimes colloquially called an accident. It is worth emphasizing, however, that the occurrence of such an event does not yet determine that it is an accident at work. Therefore, it should be referred to as an accidental event (Budzinowski, 2003).

In order for an accidental event to be considered an accident at agricultural work, it is necessary for it to meet all the conditions specified in the Act. These include the suddenness of the event, the external cause causing it and the connection of the activity performed with the agricultural activity conducted. The concept of "agricultural work" has not yet been defined by the legislator. In everyday language and in technical sciences, the term "work" appears wherever there is an action of force to overcome resistance. In this approach, we can therefore speak of the work not only of people, but also of animals (e.g. horses) and machines. Work in the economic sense is a conscious and purposeful activity of man directed at the natural environment in order to adapt it to his own needs. In this sense, work includes both physical effort (muscular work) and intellectual effort (mental work). Agricultural work - in a broader sense - will therefore be a conscious undertaking of man directed at the natural environment in order to conduct agricultural activity (Witoszko, 2005). It should be noted that the Polish legislator does not always define "agricultural activity", and the legal definitions in various legal acts are not identical. In the Insurance Act, "agricultural activity" should be understood as activity in the field of plant or animal production, including horticultural, fruit-growing, bee-keeping and fish production. In order to be able to talk about agricultural activity, it is therefore necessary to have appropriately organized instruments (an agricultural farm) and an entity that conducts this activity (an agricultural producer). The effect of this activity is primarily agricultural products. Activities related to this activity should include all activities that are aimed at producing a given product (e.g. ploughing, sowing, harvesting). However, the production process consists of various phases: from pre-production (preparatory) activities to post-production (including processing and sale of manufactured products). It is only on the market that the social and economic meaning of the activity of an entity conducting agricultural activity is realized. It should be noted, however, that this statement does not apply to social – self-sufficiency farms (Kobielski 2005).

Farm work is associated with a high risk of accidents and occupational diseases. The highest risk of accidents occurs on farms where production has a mixed profile.

The most common hazards occurring on farms include:

- mechanical hazards,
- chemical and dust hazards,

- unfavourable weather conditions,
- biological hazards,
- electrical hazards,
- noise hazards,
- falls from heights,
- welding hazards
- animal husbandry hazards (Kobielski, 2005; Salwa 2003).

The working conditions of a farmer depend to a large extent on weather conditions, but work safety depends primarily on the farmer himself, his knowledge of the hazards occurring during work performed on the farm.

5. HAZARDS OCCURRING DURING FARM WORK

*Mechanical hazards***.** These are hazards caused by mechanical elements, i.e. impacts of machines, tools, objects, animals and the ground on people, which may result in injury or death. Mechanical hazards may be caused by:

- moving machines and transported objects,
- moving working elements of machines and installations (many accidents are caused by self-designed machines, equipment and tools without appropriate guards that have been removed),
- sharp, protruding elements: buildings, structures, agricultural machinery structures, agricultural machinery and equipment tools, workshop tools,
- falling objects, materials, tools,
- during renovation of farm buildings, loading and reloading work,
- pressurized fluid, e.g. oil in the engine or hydraulic system of a lift,
- wet, uneven surfaces are a direct cause of falls. Particularly at risk are surfaces of barns and pigsties that are wet and dirty, yard surfaces in poor condition,
- muddy, slippery, poor drainage of rainwater, lack of care for the proper condition of communication routes, e.g. winter, ice, earth. A high threshold at the entrance also creates a risk of falls. Another risk of falls results from the lack of adequate lighting,
- confined spaces, i.e. in livestock buildings, especially in barns for cows and pigs, there is always a risk of injury to the operator. Similarly, where limited access to machinery or equipment creates a risk, such as crushing, it is also important to ensure adequate access,
- live animals, e.g. during work related to the breeding of bulls, boars, sows or stallions,
- various, i.e. dangerous sewage channels, cesspools, holes in the roof, improper work in the attic at height (Maszyny i inne urządzenia techniczne*…*, 2002).

Ignoring mechanical hazards, which appear at almost every step during agricultural work, can have very serious consequences. Mechanical injuries are most often crushing or amputations, e.g. of fingers or hands, bruises, stabbing or pricking, abrasions, cuts, fractures, dislocations. The direct causes of these accidents are improper gripping of tools, improper securing of machines or devices during downtime, and removing covers and guards from machines and devices (Pawłowska, 2008). It is worth remembering that the cause of mechanical hazards can be both the normal course of the work process and the action of force majeure, as well as disruptions or failures of agricultural machines. Even the correct use of machines and devices cannot always protect against hazards related to their use. The rule is that all work on agricultural equipment should be performed in accordance with the operating instructions, and access to combines and other self-propelled machines should be granted to people with appropriate qualifications and training required to operate these machines (Regulation of the Minister of Economy of 30 October 2002 on minimum requirements for occupational health and safety in the use of machinery by employees during work, 2002).

Machines must be maintained in proper technical condition, which means checking their technical condition, occasional repairs and maintenance, and cleaning parts or components of agricultural equipment, always after stopping the engine and switching off all driven elements. A farmer is more exposed than a person working in another industry to falling from a height or falling into various types of depressions. The risk of an accident is increased by the presence of agricultural machinery and other equipment, as well as dangerous sharp tools, which constitute barriers that a falling person can hit. In agricultural work, there are many situations in which falls from a height can occur, these include: renovation and construction work, stacking bulk materials during finishing, renovation, cleaning and washing work, e.g. greenhouses, trailers, agricultural machinery.

In turn, falls related to work in ditches can occur during: construction or cleaning of cesspools, deepening wells, work on silos, excavations for building foundations. In the above works, there is a high risk of mechanical injuries as a result of a fall, as well as the risk of covering people with loose material or drowning and fainting. Identification of machine hazards and the resulting dangerous situations is developed based on the analysis of activities in the work system and the way they are performed (Regulation of the Minister of Economy of 21 October 2008 on essential requirements for machines and safety elements, 2008). This analysis takes into account the time spent by work equipment in the hazard zone during normal operation (defined by the designer and/or manufacturer) under specific conditions of use, as well as the possibility of contact with factors causing mechanical hazards, such as the possibility of interference with its function and the potential consequences of such situations.

In particular, the analysis covers:

- general information describing the characteristics of the workstation, such as its location, equipment and arrangement, etc.,
- types of operations and work activities performed by operators and the manner and time of their performance,
- environmental influences on the occurrence of the examined workstation,
- other conditions in which a dangerous situation occurs (PN-EN ISO 12100).

As a result of this analysis, potential sources of injuries or other deterioration of health and dangerous situations that may lead to these effects are identified. Analysis of environmental conditions that affect the occurrence of dangerous situations at the workstation or increase the occupational risk associated with existing hazards related to machines include improper lighting (especially stroboscopic phenomena), insufficient visibility, dust, disorganized elements, spilled liquids, e.g. due to unpacked installation (PN-EN ISO 13850:2008).

*Chemical hazards***.** Chemicals are a wide range of chemical compounds with simple or complex structures that translate into their different chemical and physical properties. Of all the substances that exist, whether obtained from natural sources or by chemical synthesis, thousands are listed as hazardous chemicals. This is an open list and new entries may appear (Regulation of the Minister of Health of 30 December 2004 on occupational health and safety related to the presence of chemical factors in the workplace, 2004).

Council Directive 67/548/EEC of 27 June 1967 on the proximity of dangerous substances in laws, regulations and administrative provisions relating to classification, packaging and labelling and Directive of the European Parliament and of the Council of 31 May 1999 Council Directive 1999/ 45/EC concerning the laws, regulations and administrative provisions of the Member States relating to the classification, packaging and labelling of dangerous preparations, dangerous substances and mixtures are substances and mixtures that belong to at least one of the following classes:

- explosive substances and mixtures,
- oxidising substances and mixtures,
- extremely flammable substances and mixtures,
- highly flammable substances and mixtures,
- flammable substances and mixtures,
- alternative highly toxic substances and mixtures,
- toxic substances and mixtures,
- dangerous substances and mixtures,
- substances and mixtures corrosive,
- irritating substances and mixtures and mixtures,
- sensitizing substances and mixtures,
- carcinogenic substances and mixtures,
- mutagenic substances and mixtures and mixtures toxic to reproduction,
- substances and mixtures harmful to the environment.

They are most often found in plant protection products, fertilizers, fuel, used oils and greases and other hazardous substances used on farms, e.g. for cleaning residential premises. Plant protection products, called insecticides, destroy weeds, fungi and pests, but can also have a harmful effect on human health if they are not used and stored properly. They are among the most harmful compounds to which farmers are exposed. The high toxicity of plant protection products and their increasing use on farms mean that they pose the greatest threat to the health and even life of exposed (Regulation of the Minister of Labor and Social Policy of 29 November 2002 on the maximum permissible concentrations and intensities of harmful health factors in the work environment, 2011).

The activities that most affect farmers are: preparing solutions, such as spraying or dressing seeds, watering plants with plant protection products, cleaning and repairing sprayers. Packaging should be thrown away after work and work clothes should be washed. To reduce the risk of direct exposure to pesticides, protective clothing, gloves, appropriate footwear, goggles and respiratory protection should be worn (Regulation (EC) No. 1907/2006).

Research by the Central Institute for Labor Protection - National Research Institute (CIOP-PIB) has shown that plant protection products have a harmful effect on all important parts of the human body. According to CIOP-PIB, the level of risk posed by a pesticide is influenced by, among other things, the type of product used and its toxicity class - the most harmful are pesticides with toxicity classes I and II. However, it should be remembered that most poisonings are associated with the use of class III compounds (Council Directive 98/24/EC). Working with pesticides becomes more dangerous at elevated temperatures and humidity, especially in greenhouses – the way substances enter the body – often through absorption through the skin and respiratory system. The most exposed to pesticides were the hands, thighs, calves, forearms, eyes, face, torso and feet. These toxins can enter the body through the skin, respiratory system and digestive system. They can cause acute poisoning – when large doses are absorbed in a single dose, chronic poisoning – due to the accumulation and long-term accumulation of the drug in small doses in the body, distant poisoning – symptoms can be delayed and difficult to recognize. On the other hand, poisoning with plant protection products in small doses includes:

- poor health, general weakness,
- headache and dizziness,
- nausea, vomiting,
- abdominal pain, diarrhea,
- anxiety, agitation,
- salivation, tearing,
- sweating.

Since the symptoms are the same as food poisoning, poisoning rarely requires a doctor's visit. The most common causes of pesticide poisoning are improper use, improper storage and easy access by unauthorized persons. Good practices in the use and storage of plant protection products:

- prevent the spread of weeds, pests and pathogens through appropriate agricultural techniques,
- use integrated pest management,
- read the labels on the packaging before using plant protection products,
- properly prepare a technically efficient sprayer for work,
- properly prepare the working fluid,
- properly clean the sprayer,
- plant protection products should be stored in separate buildings or in specialist warehouses, clearly marked (with the inscription: "Plant protection products") and closed and secured against access by unauthorized persons (Regulation (EC) No. 1272/2008 of the European Parliament and of the Council).

*Dust hazards***.** The PN-ISO 4225:1999 standard defines dust as solid particles of various sizes and origins suspended in a gas for a certain period of time. The following terms can also be found in regulations and legal standards:

- total dust - a set of all particles surrounded by air in a specified volume (PN-EN 481:1998),
- fine dust - small particles of a solid; usually assumed to be particles with a diameter below 75 μm, which settle under the influence of weight, but can remain suspended for some time (PN-ISO 4225:1999),
- coarse dust - solid particles in the atmosphere or exhaust gases are harmful to humans (PN-ISO 4225:1999).
- Dust can be divided into the following groups based on the hazard:
- irritating (particles of coal, iron, glass, aluminum, barium compounds),
- fibrillating (particles of asbestos, cristobalite, tridymite, talc, iron ore and coal),
- carcinogenic substances (asbestos, special purpose refractory ceramic fibers, deciduous tree dust (beech, oak),
- allergens (dusts of plant and animal origin, pharmaceuticals, arsenic, copper, zinc, chromium dust).

The most harmful dust is produced during sharpening, grinding or polishing. Substances whose dust is considered particularly hazardous to health include primarily:

- asbestos, which is carcinogenic due to the long-term retention of fibers in the human body,
- artificial mineral fibers are often used as a substitute for asbestos,
- wood, especially oak and beech, due to its hardness,
- crystalline silica dust is considered very harmful in Poland,
- amorphous silica dust (diatomaceous earth and silica).

In agriculture, many processes produce dust, solid particles, which, after being separated from a solid body, remain suspended in the air for some time. They are the most common hazards. They are created, for example, during crushing, harrowing, threshing, cutting wood, sowing, ploughing, fertilizing, and feeding animals. The most common disease is pneumoconiosis. From the point of view of composition, the most dangerous are dusts containing silicon compounds, found mainly in asbestos, cement, hard and brown coal, talc, mineral wool and soil. The effects of exposure usually appear after many years, manifesting themselves in inflammation of the respiratory tract and cancer.

Biological hazards. According to the Regulation, harmful biological factors that can cause infection, allergy or poisoning are:

- ✓ cellular microorganisms, including genetically modified microorganisms,
- ✓ non-cellular entities capable of replicating or transferring genetic material, including genetically modified microorganisms,
- ✓ cell cultures,
- ✓ internal parasites.

The basis for the classification of biological pest factors is their impact on the health of employees. Biological factors are divided into 4 categories of hazards based on their infectivity. The criteria for classifying factors into individual groups are:

- ✓ the ability to cause disease in humans and the severity of its course,
- ✓ the probability of the disease spreading in the population,
- ✓ the probability of using effective prevention and treatment (Directive 2000/54/EC).

The condition for the occurrence of a health hazard is the entry of biological factors into the body. Biological factors can enter the body through three main routes of exposure:

- ✓ inhalation (air) - by inhaling air containing biological factors (e.g. tuberculosis, influenza, Legionnaires' disease, infectious mononucleosis, measles),
- ✓ dermal - through the skin and mucous membranes (nose, eyes) exposure to biological factors (e.g. viral hepatitis B and C),
- ✓ ingestion - by eating and/or drinking products containing biological factors (e.g. infection with the Salmonella hepatitis virus) (Dutkiewicz et al. 2007).

Biological hazards are very common in agriculture. Biological hazard factors are microorganisms and macroscopic organisms and the substances they produce, which have a harmful effect on the human body and can cause occupational diseases, especially respiratory and skin diseases. Biological hazard factors are divided into three groups:

- ✓ allergens, toxins produced by plants, such as celery, rue, etc.,
- ✓ allergens and toxins produced by bacteria, actinomycetes, fungi and animals and plants,
- ✓ infectious agents of animal origin, such as viruses, fungi and protozoa (Regulation of the Minister of Health of 28 November 2005 on the list of work positions and protective vaccinations recommended for employees taking up work or employed in these positions).

Biological factors are present in organic dust and are released in large quantities into the air inhaled by farmers. All of them have a negative impact on human health, showing toxic, irritating, sensitizing and even carcinogenic effects.

Physical hazards. Agricultural work is mainly carried out outdoors, in changeable weather. In autumn and winter, farmers are exposed to variable low temperatures and humidity, and in summer to hot conditions. High sunlight and high temperatures can significantly worsen working conditions, leading to overheating, fainting and skin lesions. Alternating work inside and outside the building is dangerous due to large fluctuations in temperature and humidity (PN-N-18002:2000).

Farmers use many electrical devices while working on the farm, and improper use can lead to accidents and illnesses. Using electrical devices can cause electric shock and burns, as well as a fire hazard (PN-N-01256-01). The premises in which farmers work are often cramped and damp, with damp and conductive floors, which further increases the risk of accidents. On the other hand, people staying for a long time near devices generating high voltage are exposed to the harmful effects of strong electric and electromagnetic fields (PN-EN ISO 14738).

On farms, there may also be hazards during the welding process. First of all, the danger of intense light radiation, thermal radiation, sparks and molten metal spatter. Depending on the type of radiation band and its wavelength, we can suffer various bodily injuries. In particular, the following may occur: inflammation of the cornea, visual impairment, retinal burns, skin burns. On the farm, we most often meet gas welders and electric welders. To prevent the harmful effects of optical radiation, eye and face protection should be used.

Noise hazard. Noise is any unwanted sound that may be bothersome or harmful to health or increase the risk of accidents at work. Noise is the most common harmful factor in the work environment. The negative impact of noise on the human body mainly concerns the hearing organ, which is the ear. Noise is also accompanied by other types of mechanical wave vibrations that may adversely affect humans. Infrasound - low-frequency vibrations (0-16 Hz), inaudible or barely audible, but strongly affecting internal organs. Ultrasound - very high-frequency waves (above 20,000 Hz), which are barely audible, but affect people, and vibrations - vibrations transmitted through solid bodies and affecting those who come into contact with them (Koradecka, 2008).

One of the most important harmful environmental factors in agriculture is noise. Farmers use machinery to work - tractors are used with complete agricultural machinery, self-propelled agricultural machinery, stationary agricultural machinery, and workshop and construction machinery. Being with animals in animal production also exposes farmers to noise. The main source of noise in agricultural environments are tractors. The Central Institute for Labor Protection - National Research Institute informs that studies of noise emitted during the operation of various machines used in agriculture have shown that agricultural tractors pose the greatest threat to the hearing organ, with the average 1-hour exposure time to noise (EA,1h) ranging from 0.05 to 4.80 (Pa2*h) depending on the type, technical condition, and manufacturer of the tractor (Engel et al. 2005; Lipowczan, 1987).

To date, studies by the Institute of Rural Medicine have only allowed determining the level of noise emitted during agricultural, transport, and workshop work. However, there have been no studies on how long farmers spend in this noise range and we do not know the true level of risk that this factor poses to farmers' health. Hearing protectors should be used at the tractor operator's position and during all other work that produces noise above the permissible level or is considered burdensome. For comparison, according to Polish law, the maximum permissible level in the A-weighted sound environment is 115 decibels, and the peak C-weighted sound level is 135 decibels. Employers must take action when noise exposure reaches 85 decibels during an eight-hour 24-hour work period - informed the National Labor Inspectorate. The tractor noise level in the cabin is about 80 decibels. Excessive and prolonged noise directly leads to fatigue, poor performance, poor concentration, disorientation, irritability, increased blood pressure, headaches and dizziness, and in the long term may lead to temporary or permanent hearing damage (Morzyński & Puto, 2005).

6. OCCUPATIONAL SAFETY IN ANIMAL PRODUCTION

There are many hazards related to accidents and diseases, both mechanical and biological, when breeding animals on a farm. The risk of mechanical accidents occurs during activities related to animals, such as milking, feeding, and sanitary procedures. Slippery floors in livestock buildings also increase the likelihood of falls. According to statistical data, in 2022, 11.2% of all agricultural accidents resulted from being hit, crushed, and bitten by animals, while 4.9% of accidents resulting from improper handling of animals, including failure to exercise special caution when handling dangerous animals, were caused by violence and aggression of animals not resulting from their biological causes (e.g. fever, first lactation, childbirth, mastitis, etc.) - 4.8% (Majchrzycka & Pościk, 2007). The data also show that in Poland about 2,000 people per year suffer injuries while working with animals, and some of them die. A particular threat to people working with animals is the risk of zoonoses. Zoonoses are infectious and parasitic diseases that people can get from sick animals or carriers of viruses, bacteria and fungi. The most common include: salmonellosis (consumption of food contaminated with feces of infected animals, especially eggs and poultry), rabies, Lyme disease and tick-borne encephalitis, tetanus, toxoplasmosis, zoonotic fungal diseases (Koradecka, 1997).

7. THE IMPORTANCE OF THE AGRICULTURAL SOCIAL INSURANCE FUND IN SHAPING SAFE WORK IN AGRICULTURE

The Agricultural Social Insurance Fund is a state institution responsible for social insurance for farmers. This system is supervised by the Minister of Agriculture and Rural Development. The Agricultural Social Insurance Fund (KRUS) is an institution that provides services to farmers in matters concerning:

- ✓ covering them with social insurance,
- ✓ paying contributions for this insurance,
- ✓ granting and paying cash benefits from insurance: retirement and disability insurance, accident insurance, sickness insurance and maternity insurance (Act of 20 December 1990 on social insurance for farmers, 2008).

Additionally, KRUS conducts preventive activities to promote the principles of work safety on farms and eliminate hazards in the workplace. The Agricultural Social Insurance Fund also conducts voluntary, free medical rehabilitation for persons entitled to benefits, at risk of incapacity for work or permanently or temporarily incapacitated to work on a farm. KRUS also performs many additional tasks assigned by the state, including:

1) pays:

- ✓ national structural pensions,
- ✓ family allowances,
- ✓ care allowances,
- ✓ veterans' benefits for war invalids,

2) manages the health insurance of farmers, their household members, retirees and pensioners, members of their pensioner and pensioner families, while also acting as a payer of contributions for this insurance on behalf of the National Health Fund (Puślecki, D. 2006).

In the social insurance of farmers, two types of insurance operate on separate financial principles:

- ✓ pension and disability insurance, financed mainly from a budget subsidy, supplemented by income from contributions from insured farmers,
- ✓ accident, sickness and maternity insurance, the implementation of benefits from this insurance is guaranteed only by contributions from farmers, collected in the Contribution Fund of the Social Insurance of Farmers. This fund is a legal person, the functions of the management board are performed ex officio by the President of KRUS, under the supervision of the Farmers' Council.

The organizational structure of KRUS consists of:

- ✓ Headquarters
- ✓ 16 regional branches,
- ✓ 256 local branches.

The Agricultural Social Insurance Fund is managed by the President as the central public administration body subordinate to the minister responsible for agriculture. The President of the Fund is appointed and dismissed by the Prime Minister, upon an application submitted after seeking the opinion of the Council of Farmers. Under Article 76 of the Act on Social Insurance for Farmers, the President of KRUS performs ex officio, under the supervision of the Council of Farmers, the functions of the board of the Contribution Fund of the Social Insurance for Farmers (Jędrasik-Jankowska, 2002). The monthly amount of the contribution to retirement and disability insurance is 10 percent of the basic pension. The amount of the basic pension is announced by the President of ZUS in the Official Journal of the Republic of Poland "Monitor Polski" (Salwa, 2003).

The basis for financing all statutory tasks of KRUS are three state earmarked funds: the Pension and Disability Fund, the Prevention and Rehabilitation Fund, the Administrative Fund, and also the extra-budgetary Contribution Fund of the Social Insurance for Farmers.

8. ACCIDENT RATE AND PREVENTIVE MEASURES

The basic machine used in agricultural work is the tractor. Used with machines cooperating during field work and for transport work, it facilitates work, increases efficiency and allows for cost reduction, but it is also a machine that poses the greatest threat to the health and life of farmers operating it. The operation of machinery and safety depend largely on its skillful operation. Every year, over 20,000 accidents occur on individual farms, resulting in dozens of deaths (Solecki, 2008). According to KRUS data, the structure of accidents has not changed significantly in recent years, and the causes of most injuries are: "falls", "being caught or hit by moving parts of machines and devices" and "being hit, crushed" or bitten by animals. A large number of accidents occurred during the use of agricultural machines in the logistics and production process. The largest share of machines in accidents were agricultural tractors, trailers, combines and means of transport (Puślecki, 2011).

There are many causes of agricultural accidents and they are related to the specificity of farmers' work, characterized by a lack of time frames, variable working conditions, multitasking, the presence of children and animals in the work environment. The work is characterized by excessive physical and mental consumption, the use of many generally outdated machines and technical devices (Jaworski, 2007). The most common accidents during agricultural work include falls, dropped objects, being caught and hit by moving parts of machines, crushing, biting and other events involving animals (kick, hit, knocked over by an animal) and the forces of nature (extreme temperatures, storms, cyclones, etc.) (Puślecki, 2010). According to the Institute of Rural Medicine, the most common forms of this are: broken bones, cuts, bruises, sprains, burns, crushing (amputation), etc. Therefore, in agriculture, farmers are exposed to a very high occupational risk in the form of agricultural accidents and agricultural occupational diseases. KRUS data do not reflect the actual number of agricultural accidents in Poland, because some farmers do not apply for insurance. The current law includes two types of insurance:

- ✓ full (against the consequences of accidents on the farm),
- ✓ limited (against the consequences of accidents outside the farm, which covers only accidents occurring during normal activities related to agricultural activity or in connection with conducting such activity) (Puślecki, 2011).

The interpretation of the concept of accidents at agricultural work was initially difficult due to the lack of statutory definition of agricultural work and the introduction of broader concepts (Kobielski, 2005). The concept of agricultural activity falls within the definition of an accident, which is too narrow in agricultural law, because it excludes preparatory and organizational activities and activities in the post-production phase. Only when three elements are met simultaneously: suddenness of the event, externality of the cause and connection with work, can we speak of the existence of accidents at work in the legal sense. In order for an event to be considered sudden, the factors that caused it must affect the victim within a short time (Rodak, 2012). However, the concept of transience is not clearly defined as time, the decisive criterion here is not so much the short duration of the event, but the lack of time for the victim's consciousness to register the state of danger, for the victim to be able to take precautions and prevent it. If the accident occurred at home or on a farm, any such accident can be considered an accident at agricultural work if it is related to activities related to conducting agricultural activity or performing such activities. In addition, there must be a temporal and functional connection with agricultural work, but we are not dealing here with a classic, fully causal form of relationship. The combination of "local" and "functional" relationships is characteristic here. Accidents are sudden events caused by external causes, occurring outside the farm and home and its premises, while performing "everyday activities related to agricultural activity" (Jędrasik-Jankowska, 2003). This also applies to farmers who have accidents while picking fruit from trees and, as a farmer, have accidents on neighboring farms as part of neighborly help. The problem of many accidents at work that are not recognized as accidents on farms results from the fact that the definition of "accident" is imperfect. The correct construction of the legal concept of "agricultural accident" is of fundamental importance for the protection of victims of accidents (Szymanek & Zarychta, 2004).

The specificity of agricultural work is characteristic enough to justify special protection of farmers and members of their families against accidents and diseases related to agricultural work. Social insurance for farmers should therefore provide adequate and broad protection for people working in agriculture (Puślecki, 2006). The main goal of preventive measures implemented by KRUS local units is to disseminate the "Principles of health and life protection on a farm", which are recommendations regarding the equipment of a farm, protection of people working on it and the method of performing activities related to agricultural activity (Accidents at work and occupational diseases of farmers and preventive measures of KRUS in 2020, 2021). The content of the document was first published in 1995 and then amended in 2008 and 2020, in accordance with the arrangements of the President of the Fund in agreement with the Council of Farmers and ministers responsible for health, social protection and rural development. The need for updating results from the need to adapt individual regulations to the statutory and regulatory provisions and good agricultural practices in force in EU countries (Szewczyk, 2005). The latest edition contains advice on work organization, environmental protection, fire protection, handling hazardous substances (such as plant protection products, fuels and fertilizers), as well as on the psychophysiological state of farmers and their health. The dissemination of these principles is the main goal of preventive activities of KRUS units. The Act on the Social Insurance of Farmers indicates that claims can be made from suppliers of agricultural products and services whose defects are the only or main cause of accidents at work in agriculture or occupational diseases, for monetary compensation from insurance paid to injured farmers (Szewczyk, 2006).,

Based on the analysis of the causes and circumstances of accidents and occupational diseases reported to KRUS in 2020, the President of the Fund determined the following directions of KRUS preventive actions:

a) dissemination of the updated "Principles of health and life protection on a farm" and the "List of particularly dangerous activities related to running a farm, which must not be entrusted to children under 16 years of age" among farmers, their families and children of people associated with the rural environment,

b) influence the elimination of hazards and prevent the most common accidents from the following groups: falling people, being caught and hit by moving parts of machines and devices, being hit, crushed and bitten by animals, falling objects and other accidents. This is done by popularizing:

- ✓ improving the surface of yards and communication routes on the farm
- ✓ using work safety measures
- ✓ using platforms and ladders to prevent tipping and sliding during work at heights,
- ✓ eliminating thresholds and failures in buildings and communication routes,
- ✓ the correct method of getting on and off agricultural machinery,
- ✓ ensuring that machinery is equipped with guards and that its moving parts are secured,
- ✓ properly securing machinery and tools when stationary and in motion,
- ✓ applying the principle of safe timber harvesting for the needs of the farm,
- ✓ taking care of the farmer's appropriate mental state (healthy lifestyle, diagnostics),

c) influencing the proper production and distribution of agricultural products and protective measures by:

- ✓ informing farmers about products marked with the KRUS Safety Mark and the distinction awarded by the President of KRUS entitled A product that increases work safety on a farm and encourages its purchase and use,
- ✓ a preventive and recourse program aimed at eliminating from the market products with structural defects that may cause accidents or pose a threat to users,
- ✓ informing farmers about ways to prevent occupational diseases - mainly about preventing tick bites and the rules of conduct in the event of a bite,

- ✓ familiarizing farmers with the basic rules of conduct and methods of providing first aid in the event of an accident (Accidents at work and occupational diseases of farmers and preventive activities of KRUS in 2021, 2022).

The President of the Fund instructs the heads of local branches to supervise the proper determination of the cause and circumstances of the accident and to conduct preventive measures in accordance with the Act on Social Insurance for Farmers (Jędrasik-Jankowska, 2013).

9. CONCLUSION

In order to provide people with the best possible living conditions, Poland spares no effort to create the most favorable working conditions possible. This aspiration is reflected in the Constitution of the Republic of Poland. In addition, a number of legal acts oblige employers to organize production processes in such a way that they do not threaten the health and life of employees.

The state's activity in this area is based on specific organisational principles. The employees themselves and their social organisations, state and local government administration and scientific institutions take an active part in creating safe and harmless working conditions.

A new organisational system for labour protection has been created in Poland, which consists of three main divisions: executive, supervision (inspection) and scientific and research. Each of them has its own specific tasks, and the harmonised activity within these three divisions ensures the implementation of a common goal, which is to create safe and harmless working conditions. A characteristic feature of this system is the close connection between the executive division, which is in the hands of the state administration, and the supervision division, the core of which are employees.

In Poland, the obligation to comply with occupational health and safety regulations and to apply safe work principles has been imposed on all employees. The management body of the workplace, appointed to perform specific occupational health and safety tasks and at the same time having the right to control compliance with occupational health and safety regulations, is the workplace administrative occupational health and safety service. This is particularly important in the field of agriculture, where various types of accidents and unfortunate events very often occur during the performance of various types of work.

REFERENCES

Bińczycka-Majewska, T. (1993). *Prawne aspekty chorób* zawodowych, „Państwo i Prawo", z. 7, s. 52-56.

Budzinowski, R. (2003). *Prawne pojęcie działalności rolniczej*, „Prawo i Administracja" , t. II, s. 167.

Cież, J. (2013), *Bezpieczna praca w rolnictwie. Pracuje bezwypadkowo,* Instytut Medycyny Wsi, Lublin 2013, s. 61.

Puślecki, D. (2004) *Z rozważań nad pojęciem wypadku przy pracy rolniczej*, [w:] R. Budzinowski (red.), *Problemy prawa rolnego i ochrony środowiska*, Poznań, s. 198.

Dutkiewicz, J., Śpiewak, R., Jabłoński, L. & Szymańska, J. (2007). *Biologiczne czynniki zagrożenia zawodowego. Klasyfikacja, narażone grupy zawodowe, pomiary, profilaktyka*, Ad Punc tum, Lublin.

Dyrektywa 2000/54/WE z dnia 18 września 2000 r. w sprawie ochrony pracowników przed ryzykiem związanym z narażeniem na działanie czynników biologicznych w miejscu pracy.

Dyrektywa Rady 98/24/WE z dnia 7 kwietnia 1998 r. w sprawie bezpieczeństwa pracowników oraz ochrony ich zdrowia przed ryzykiem związanym z czynnikami chemicznymi podczas pracy.

Engel, Z., Piechowicz, J., Pleban, D., & Stryczniewicz, L. (2005). *Minimalizacja przemysłowych zagrożeń wibroakustycznych - Poradnik*, Centralny Instytut Ochrony Pracy, Warszawa, s. 56.

Jaworska-Spicak, E. (2001). *Choroba zawodowa a prawo do jednorazowego odszkodowania dla rolnika*, „Ubezpieczenia w Rolnictwie. Studia i Materiały", nr 1, s. 94.

Jaworski, H. (2007) *Wypadki przy pracy i choroby zawodowe rolników oraz działalność* prewencyjna KRUS w 2006 roku, „Ubezpieczenia w Rolnictwie. Studia i Materiały", nr 31, s. 7-26.

Jędrasik-Jankowska, I. (2002). *Ubezpieczenia wypadkowe i chorobowe*, Warszawa, s. 61.

Jędrasik-Jankowska, I. (2003). *Ubezpieczenie społeczne*, t. III: *Ubezpieczenie chorobowe. Ubezpieczenie wypadkowe*, Warszawa, s. 148.

Jędrasik-Jankowska, I. (2013). *Pojęcia i konstrukcje ubezpieczenia społecznego*, Warszawa, s. 421.

Kobielski, W. (2005). *Wypadki przy pracy i choroby zawodowe rolników-wybrane problemy*, „Ubezpieczenia w Rolnictwie. Studia i Materiały", nr 2, s. 30.

Koradecka, D. (Ed.) (1997). *Bezpieczeństwo pracy i ergonomia*, Centralny Instytut Ochrony Pracy, Warszawa 1997, s. 37.

Koradecka, D. (Ed.) (2008). *Bezpieczeństwo i higiena pracy*, Centralny Instytut Ochrony Pracy – PIB, Warszawa, s. 56.

Lipowczan, A. (1987). *Podstawy pomiarów hałasu, wydanie pierwsze*, Główny Instytut Górnictwa, Katowice-Warszawa, s. 67.

Majchrzycka, K., & Pościk, A. (Ed.) (2007). *Dobór środków ochrony indywidualnej,* Centralny Instytut Ochrony Pracy - PIB, Warszawa, s. 67.

Maszyny i inne urządzenia techniczne. Środki ochrony przed zagrożeniami mechanicznymi, Warszawa, CIOP 2002.

Miłkowski, W., Nasternak, E., Król, M. & Kucharska, B. (2014). *BHP w rolnictwie dobre praktyki w gospodarstwach rolnych,* FAPA, Warszawa, s. 41.

Morzyński, L. & Puto, D. (2005). *Hałas w środowisku pracy*, Państwowa Inspekcja Pracy, Warszawa, s. 56.

Norma PN-ISO 4225:1999.

Pac, W. (2006). *Dynamika przeobrażeń samorządowych w aspekcie kreowania podmiotowości jednostek i grup społecznych*. Seminare. Poszukiwania naukowe, 23(1), 195-212.

Pac, W. (2018). *Służby specjalne w sferze bezpieczeństwa państwa. Człowiek - społeczeństwo - bezpieczeństwo*, Wyd. Państwowa Wyższa Szkoła Wschodnioeuropejska w Przemyślu, 42-58.

Pac, W. (2022). *Prawne i instytucjonalne uwarunkowania ścigania przestępstw przerzutu imigrantów przez wschodnią granicę Rzeczypospolitej Polskiej jako zewnętrzną granicę Unii Europejskiej.* Przegląd Policyjny, 147(3), 224-239.

Pac, W. (2023). *Legal and Institutional Conditions for Prosecuting Smuggling of Immigrants Across the Eastern Border of the Republic of Poland as an External Border of The European Union.* Przegląd Policyjny, 147, 224-239.

Pac, W. (2024a). *Demographic and social consequences of the Russo-Ukrainian war for Ukraine*. Politics & Security, 9(3), 53–67.

Pac, W. (2024b). *Humanitarian assistance for war refugees from Ukraine: A case study of the Podkarpacki Branch of the Polish Red Cross.* Politics & Security, 9(3), 36–52.

Pac, W. (2025). *Challenges and strategies in Poland's policy towards Ukraine in the context of migration.* Politics & Security, 11(1), pp.42–54.

Pawłowska, Z. (2008). *Podstawy prewencji wypadkowej*, Warszawa, CIOP - PIB.

PN-EN ISO 12100 (norma arkuszowa) *Bezpieczeństwo maszyn - Pojęcia podstawowe, ogólne zasady projektowania.*

PN-EN ISO 13850:2008 *Bezpieczeństwo maszyn – Stop awaryjny - Zasady projektowania* (oryg.)

PN-EN ISO 14738 Maszyny - Bezpieczeństwo - Wymagania antropometryczne dotyczące projektowania stanowisk pracy przy maszynie.

PN-N-01256-01: Znaki bezpieczeństwa – Ochrona przeciwpożarowa.

PN-N-18002:2000 Systemy zarządzania bezpieczeństwem i higieną pracy Ogólne wytyczne do oceny ryzyka zawodowego.

PN-N-18002:2011 *System zarządzania bezpieczeństwem i higieną pracy. Ogólne wytyczne do oceny ryzyka zawodowego.*

Praktyczne wytyczne o charakterze niewiążącym w sprawie ochrony zdrowia i bezpieczeństwa pracowników przed ryzykiem związanym ze środkami chemicznymi miejscu pracy; Komisja Europejska, Dyrekcja Generalna ds. Zatrudnienia, Spraw Społecznych i Równości Szans.

Puślecki, D. (2006). *Z problematyki prawnej wypadku przy pracy rolniczej*, „Prawo i Administracja", nr 5, s. 325-342.

Puślecki, D. (2010). *Nowy model społecznego ubezpieczenia wypadkowego rolników*, „Przegląd Prawa Rolnego", nr 2, s. 79.

Puślecki, D. (2011) *Społeczne ubezpieczenie wypadkowe rolników. Zagadnienia* prawne, Warszawa – Poznań, s. 119.

Puślecki, D. (2011). *Pojęcie wypadku przy pracy rolniczej – uwagi de lege ferenda*, „Przegląd Prawa Rolnego", nr 2, s. 66-67.

Puślecki, D. 2006. *Z problematyki prawnej wypadku przy pracy rolniczej*, „Prawo i Administracja", t. V, s. 325

Rodak, K. (2012). *Kształtowanie się pojęcia wypadku w ubezpieczeniu społecznym rolników*, „Ubezpieczenia w Rolnictwie. Studia i Materiały", nr 45, s. 50.

Rozporządzenie (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniające dyrektywę 1999/45/We oraz uchylające rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE (Dz. U. UW z dnia 30 grudnia 2006 r.).

Rozporządzenie Ministra Gospodarki z dnia 21 października 2008 r. w sprawie wymagań zasadniczych dla maszyn i elementów bezpieczeństwa, (Dz. U. nr199, poz.1228) - transponuje do prawa polskiego dyrektywę 2006/42/WE tzw. maszynową.

Rozporządzenie Ministra Gospodarki z dnia 30 października 2002 r. w sprawie minimalnych wymagań dotyczących bezpieczeństwa i higieny pracy w zakresie użytkowania maszyn przez pracowników podczas pracy, (Dz.U nr 191, poz. 1596, zmiana Dz . U 2003, nr 178, poz. 1745).

Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 29 listopada 2002 r. w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy (Dz. U. z 2002 r. Nr 217, poz. 1883 ze zmiana mi oraz z 2011 r. Nr 274 poz. 1621).

Rozporządzenie Ministra Zdrowia z 22 kwietnia 2005 r. w sprawie szkodliwych czynników biologicznych dla zdrowia w środowisku pracy oraz ochrony zdrowia pracowników zawodowo narażonych na te czynniki (Dz. U. Nr 81, poz. 716 z późn. zm.

Rozporządzenie Ministra Zdrowia z dnia 28 listopada 2005 r. w sprawie wykazu stanowisk pracy oraz szczepień ochronnych wskazanych do wykonywania pracownikom podejmującym pracę lub zatrudnionym na tych stanowiskach (Dz. U. z 2005 r., Nr 250, poz. 2113).

Rozporządzenie Ministra Zdrowia z dnia 30 grudnia 2004 r. w sprawie bezpieczeństwa i higieny pracy związanej z występowaniem w miejscu pracy czynników chemicznych (Dz. U. z 2005 r. Nr 11, poz. 86 oraz z 2008 r. Nr 203, poz. 1275).

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1272/2008 z dnia 16 grudnia 2008 r. w sprawie klasyfikacji, oznakowania i pakowania substancji i mieszanin, zmieniające i uchylające dyrektywy 67/548/EWG i 1999/45/WE oraz zmieniające rozporządzenie (WE) nr 1907/2006.

Salwa, Z. (2003). *Pojęcie wypadku przy pracy*, „Praca i Zabezpieczenie Społeczne", nr 3, s. 19.

Solecki, L. (2008). *Stres w pracy i życiu rolnika -jego skutki zdrowotne*, „Ubezpieczenia w Rolnictwie. Studia i Materiały", nr 32, s. 15-22.

Szewczyk, H. (2005). *Prawne problemy wypadków przy pracy i chorób zawodowych w rolnictwie*, [w:] *Z problematyki prawa pracy i polityki socjalnej*, t.16, red. A. Nowak, Katowice, s. 152.

Szewczyk, H. (2006). *Stres jako przyczyna wypadku przy pracy*, „Praca i Zabezpieczenie Społeczne", nr 6, s. 31-38.

Szymanek, T., & Zarychta, W. (2004). *Wypadki przy pracy i dochodzenie roszczeń*, Warszawa, s. 35.

Ustawa z 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników, tekst jedn.: Dz. U. 2008, Nr 50, poz. 291 ze zm., (dalej jako: ustawa ubezpieczeniowa).

Ustawa z dnia 25 lutego 2011 r. o substancjach i ich mieszaninach (Dz. U. z 2011 r., Nr 63, poz. 322 ze zm.) stan prawny na 01.07.2013 r.

Witoszko, W. (2005). *Pojęcie stałego i długotrwałego uszczerbku na zdrowiu w razie jednorazowego odszkodowania z tytułu wypadku przy pracy*, „Monitor Prawa Pracy", nr 5**,** s. 124.

Wyka, T. (2001). *Bezpieczeństwo i ochrona zdrowia pracowników w działalności normotwórczej* MOP, PiZS, nr 12, s. 32.

Wypadki przy pracy i choroby zawodowe rolników oraz działania prewencyjne KRUS w 2020 roku, KRUS Warszawa 2021, s. 21.

Wypadki przy pracy i choroby zawodowe rolników oraz działania prewencyjne KRUS w 2021 roku, KRUS Warszawa 2022, s. 22-23.

Bairagi, L., Harun-Ar-Rashid, M., Rahman, S. M., Sheikh, T., & Hossain, T. (2025). Exploring the influence of economic and environmental knowledge on fish production in rural Bangladesh. Politics & Security, 12(2), 32–40.
Doi: 10.54658/ps.28153324.2025.12.2.pp.32-40

EXPLORING THE INFLUENCE OF ECONOMIC AND ENVIRONMENTAL KNOWLEDGE ON FISH PRODUCTION IN RURAL-BANGLADESH

Linda Bairagi
Sub Assistant Land Officer, Khulna
Khulna, Bangladesh
bairagilinda@gmail.com
https://orcid.org/0009-0009-2790-8776

Md. Harun-Ar-Rashid
Divisional Cooperative Office
Khulna, Bangladesh
haruncooperative41@gmail.com
https://orcid.org/0009-0004-9965-7578

Sk. Mahrufur Rahman
Department of Business Administration, North Western University
Khulna, Bangladesh
mahrufur89@gmail.com
https://orcid.org/0009-0005-0200-1933

Tanjila Sheikh
District Manager, BRAC
Satkhira District, Bangladesh
sheikhoaishi94@gmail.com
https://orcid.org/0009-0003-0379-3421

Tanbir Hossain
Department of Economics, North Western University
Khulna, Bangladesh
tanbir.nwustu@yahoo.com
https://orcid.org/0000-0003-1935-3001

Abstract *Aquaculture is a buzzword for rural economy as well as regional development. In this research, the author considers five individual villages where 200 farmers have been identified randomly. In this paper, the author divides this research into two segments. Firstly, most of the local farmers consider basic factors, where variable costs that is daily basis expenses affect fish production variables for farmers. Secondly, the authors try to identify the environmental knowledge index (EKI) for farmers affecting fish production, the EKI is measured by table 2. In Table 3, most of the expenses are calculated for human labor, fish feed and fingerlings purposes. Marginal farmers face higher variable costs compared to the other two categories of farmers. The authors run the Cobb-Douglas multiple regression model to investigate the effect of independent variables on fish production hectare-wise, while human labor cost, feed and manure cost, water supply, and Sustainability knowledge index have positive and significant relationships with fish production. To justify the 2nd research question, EKI has a significant connection with fish production for farmers,* *because EKI helps farmers to lead production at a lower cost while maintaining a hygienic production system. The green economy is the upcoming challenge for the future, which leads to sustainable production and consumption behavior for producers and consumers. Moreover, sustainable and effective marketing channel creation are challenging factors for fish production and supply.*

Keywords Aquaculture, Marginal-farmers, Environmental Knowledge, Green economy, Rural-Bangladesh.

1. INTRODUCTION

Bangladesh stands out as an effective and handy player in global fish production divided into three main categories inland capture, inland fish production culture and marine fisheries. In the fiscal year 2021-2022, fish production rises up to 47.59 Metric tons where aquaculture contributes almost 57.39% (DoF, 2022). In recent times, it has been observed that aquaculture practices are closely connected with paddy production which systematically transformed into an aquaculture system on a full-time basis in Bangladesh (Ahmed et al., 2011; Deb et al., 2013; Mondal, 2008). In the fiscal year 2021-2022, the fishery sector expanded to GDP growth of about 2.08% while agro-sectors stood at about 21.83% (BER, 2022) because about 12% population connects directly or indirectly with aquaculture sectors that reach our homeland as 3rd position for global overview. From the perspective of carp-fish production, Bangladesh stands as 3rd in Asia, furthermore, Bangladesh produces Hilsa fish (National Fish of Bangladesh) and holds 11.91% of total fish production (DoF, 2022).

Aquaculture plays a significant role in food security and poverty alleviation approaches worldwide because of its capacity to produce freshwater fish, which, while it consists of low-value species in consideration of market valuation, provides food items and increases nutritional variety all over the planet. Aquaculture could play a chief role in meeting the needs of people in terms of food now and in the future generations where freshwater fish farming or aquaculture plays an effective role in developing livelihood patterns of rural people in Bangladesh (Mazid, 2002). It develops various livelihood opportunities for several people all over the world who are living below the poverty level, in the figure of farmers, market operators, employees, fish traders, middlemen, daily labourers and transporters connected with fish-trading (Ahmed & Rahman, 2004). Moreover, Bangladesh has achieved its self-sufficiency for inland fish production taking the core support of government and non-governmental support, where Bangladesh is producing about 43.48 Lac metric tons of fish considering the demand of 40 Lac MT fishes, Likely 62.58 grams of fish consumed as nutrition against the daily consumption level of 60 grams fishes reported by (DoF, 2018).

Aquaculture stands out as the most rapidly growing sector for fish production, it has proven a profitable and effective role in meeting the nutritional and livelihood needs of local people (Hasan & Jahan, 2022). It is reported that global aquaculture is producing 80 million total fish consisting of 47% world fisheries production and capture (DoF, 2016), where global fish production has surged by about 179 million tons of total capturing fish divided by capture fisheries (96.4 million tons) and aquaculture (82.1 million tons (FAO, 2020). Aquaculture contributes half a portion of total fish production and is proven as the swiftest growing sector for ensuring food security with proper nutritional balance (Singha & Chandan, 2023). In recent times, it has been noticed that Bangladesh, India, China, Myanmar, Indonesia, and Cambodia are trying to connect their inland for professional aquaculture production to accelerate economic wheels (FAO, 2020).

2. MATERIALS &METHODS

Bangladesh is well-known as a riverine country where rivers are being used as professional methods of communication, economic development and development of livelihood patterns from root level to top. Moreover, the northeastern region of Bangladesh, Hakaluki Haor and Tanguar Haor, is recognized as the heart of generating natural fish-breed that maintains fish ecology mostly (Kumar et al., 2022). These areas cover 40,000 hectares of northeastern regions like (Sunamganj, Moulvibazar etc) and play effective roles in ecological and social spheres (Tamim et al., 2022). These regions are the most important part connecting to the aquaculture industry for livelihood earning, employment generation, irrigation systems, fodder and transportation. Basically, these regions help to maintain effective factor biodiversity and natural balance (Sarker & Alam, 2023). The regional benefits help to produce natural fish for Bangladesh and revitalize the fish industry at a large scale supporting national GDP (DoF, 2022). In recent report identifies that most parents discourage their children not to engaging in this traditional culture because of the generation gap, and send them to aboard for a glorious life (Ghose, 2017).

This culture breaks down the point of passion connecting with aquaculture which hampers continued fish production in the northern part of Bangladesh. Shamsuzzaman et al. (2017) highlighted that Bangladesh has been considered the most demandable and advanced land for flooded wetlands and large bio-diversified aquatic factors in the Asian belt after considering the giant China and India: Aquatic development has been possible due to the huge demand for protein, food efficiency, earning large volume of foreign-currency, improving life standard, declining poverty, local and regional development factors. Supporting these statements, paddy farming is converting to fish cultivation overdue time being the most profitable sector (Islam et al., 2002; Islam et al., 2017).

According to the report of FAO (2020), a prime portion of aquaculture fish production happens in Asian countries where these countries have been able to produce almost half portion of total fish exports, China, Indonesia, India, Viet Nam and Bangladesh are at the top five exporter countries in the world where aquaculture is proved as spinal-strength for local people. Bangladesh is now graded 5th in the world aquaculture production (FAOSTAT, 2016). Aquaculture practice has a high positivity to achieve self-sufficiency for ensuring food security and diminishing poverty from a Bangladeshi economic perspective (Al-Amin et al., 2012). A lot of factors are intentionally engaged with fish production, these are water supply, seasonal variation, fish-feed price, government and non-governmental supports, fish-fry supply at proper time etc. FAO (2013) mentioned that China is the leader for large volume fish-exporting which covers most of the protein sources for Chinese people. In economic review, Bangladesh is sanctified with inland water sources like ponds, haor, baor and lakes that cover about 5488 hectares, covers huge aquaculture sectors (DOF, 2015). Following this statement, it is observed that farming technology, species-generation, and fish breeding are the major sources of fish production that covers 41.34 lac MT, covering about 56.44% of total fish production (DoF, 2018). In a recent report, Bangladesh achieved 5th rank in world fish production, both Aquaculture and fisheries tackle almost 25.30% figure of the total GDP covering 3.57% national GDP (FAO, 2016). From Bangladesh's perspective, about 11% of the total population is connected with the fishery sector to survive their livelihood (DoF, 2018).

According to the report of FAO (2018), Bangladesh has been covered with 260 freshwater sources where biodiversity is being maintained by different types of flora and fauna. To chase the SDG by 2030, it is high time to maintain green agriculture where it declines carbon emission levels at the maximum level. Within all fish items, Hilsa fish needs to maintain a high chain of biodiversity that covers approximately 12% of total inland fish production.

According to the report of Ferdoushi et al. (2019), Tilapia fish production has been proven most profitable business in the north-eastern part of Bangladesh, The average total cost per hectare is 0.33 million for tilapia monoculture compared to tilapia culture (0.241) million. So, the net margin is higher for tilapia monoculture which is 1.51 based on the cost-benefit ratio. Ebukiba et al. (2019) carried out a research study on the economic investigation of catfish production in the Karu local government area of Nasarawa State, Nigeria, that is proved a profitable business for the Nigerian economic perspective. Shawon et al. (2018) highlighted a paper on the socio-economic position and financial productivity of small-scale shrimp farming in coastal areas of Bangladesh, small scale farmers are economically profitable due to regional advantage.

Busari (2018) investigated an economic analysis of the farmstead aquaculture system in the Olorunda local government area, Osun State, Nigeria, which focuses on middle-aged, catfish farmers specially to focus the research. The researchers analyzed that the GM and RRI are 475,342.51 and 468,451.18 Nigerian currency (Naira) respectively supporting the return of 71.02% profit in the study area. Moreover, Bangladesh exports its fishery products to more than 55 countries, where the European Union is the major hub (Shamsuzzaman et al., 2017). However, Bangladesh is considered as still a trade-deficit country in terms of its fishery resources which is contradictory to the motion of the country. In Bangladesh, there is an apparent difference between the inland and marine fisheries production trend from FY'1984-85 to FY'2018-19 (Sunny et al., 2021). The trend of freshwater fisheries yields from 2007 to 2019 presents a production gap between freshwater capture and freshwater culture (Hasan et al., 2021).

The influence of the fisheries sector was 2.54% of the GDP of Bangladesh in 2021 (Manik, 2023). Either directly or indirectly, nearly 12% of the country's population depends on fisheries and aquaculture-related activities for their livelihood pattern (Department of Fisheries, 2020). The long-term Climate Risk Index expresses a 28.3 score that ranks Bangladesh seventh among the tenth most affected countries in the world due to climate change effect (Eckstein et al., 2021). About 90% of global aquaculture is supplied by developing countries which are measured global climate risk as hotspots (Islam et al., 2019). Overpopulation effect and climate change are the main difficulties in Bangladesh.

2.1 RESEARCH METHODOLOGY

This study is mainly based on primary survey which is based on simple random sampling. The author selects 5 villages where most farmers are engaged with aquaculture. The author selects five villages named *Chachibunia, Chokrakhali, Kochubunia, hatbati, Hogolbunia, taking 40 fish farms from every village for fish 200 farms.*

2.1.1 Cobb- Douglas Production Function

This function was used to estimate the effects of various inputs for the production of Koi fish. The functional form of the Cob-Douglas multiple regression equation was as follows.

$$\mathbf{Y = a+X1\ b1 +X2\ b2 +X3\ b3+ X4\ b4 + X5\ b5+ X6\ b6 +X7\ b7 +X8\ b8 +X9\ b9+ X10\ b10+ u.}$$

The equation may be alternatively expressed in log-linear form:

$$lnY = lna + b1lnX1 + b2lnX2 + b3lnX3 + b4lnX4 + b5lnX5 + b6lnX6 + b7lnX7 + b8lnX8 + b9lnX9 + b10lnX9+ U$$

Table 1: Estimation of Variables with Expected Sign for Fish Production

S.N	Variables Name	Variable Sign	Measurement Scale	Expected Sign	Literature References
1.	Human labor cost	*X1*	BDT/ Hectare	+	Ele et al. (2013); El-Naggar et al. (2008)
2.	Fingerling cost	*X2*	BDT/ Hectare	+	Ebukiba & Anthony (2019)
3.	Feed cost	*X3*	BDT/ Hectare	+ or -	Faruk (2003)
4.	Manure cost	*X4*	BDT/ Hectare	+	Faruk (2003)
5.	Fertilizer cost	*X5*	BDT/ Hectare	+ or -	Faruk (2003)
6.	Lime cost	*X6*	BDT/ Hectare	+ or -	Ferdoushi et al. (2019)
7.	Pesticide cost	*X7*	BDT/ Hectare	+	Islam (2002)
8.	Water supply cost	*X8*	BDT/ Hectare	+	Islam (2002); Islam (2008)
9.	Electricity cost	*X9*	BDT/ Hectare	-	Itam et al. (2014)
10.	Environmental Knowledge	*X10*	Index Score	+ or -	Author Own Compilation

Dependent Variable: Hectare wise Fish Production

Source: Authors Own compilation, 2025

2.2.2 Efficiency of Resource Allocation

In order to test the efficiency, the ratio of Marginal Value Product (MVP) to the Marginal Factor Cost (MFC) for each input was computed and tested for its equality to 1.

$$\mathbf{ERA:}\ \frac{\mathbf{MVPx}}{\mathbf{MFCx}} = \mathbf{1}$$

From the above equation, it is seen that The marginal productivity of a particular resource represents if the owner increases 1 unit of input for fish-farming, how much he will get as output considering all others input as constant. The addition to gross returns in value term produced by an extra 1 unit of that resource, while other inputs are held constant. The most dependable, perhaps the most useful, estimate of MVP is achieved by taking fish-resources value as gross outcome at following geometric means (Islam, 2008). In terms of farming, Marginal Factor Cost (MFC) means the input valuation spent for fish-farming to gain effective outputs.

Table 2: Estimation of Environmental Knowledge Index (EKI)

Indicators	**Scoring Index**	**Required Score**
Knowledge about Greenhouse Effect	1 to 5	Very Low=1, Low=2, Moderate = 3, Good=4, Very Good=5 ***(Minimum Score=6 and Maximum Score =30)***
Knowledge about toxic creation from pond	1 to 5	
Awareness about Eco-friendly Fish-feed	1 to 5	
Responsible Knowledge of Carbon Emission from Pond	1 to 5	
Knowledge about Environmental-friendly Fertilizer usage	1 to 5	
Knowledge about Water Wastage Management	1 to 5	

Source: Authors Own compilation, 2025

3. RESEARCH RESULT

Profitability is the chief aim of any farmer. In order to earn a respectable economic return, production cost becomes an important factor and accordingly it contributes a dominant role for farmers. Costs and returns are valued on the basis of authentic market prices affected by the fish-farmers.

Table 3: Per Hectare Costing of Producing Different Categories of Fishes
(Hectare wise BDT Costing per Year)

Cost items	**Marginal farmers**	**Small farmers**	**Medium farmers**
Variable cost			
Human labor	4,67,130	4,25,228	3,83,450
	(20.36)	*(14.86)*	*(11.45)*
Feed	11,50,214	15,80,567	18,62,513
	(62.05)	*(70.45)*	*(74.45)*
Fingerlings	1,60,233	1,70,487	1,75,502
	(8.67)	*(6.97)*	*(6.36)*
Fertilizer	18,908	15,737	16304
	(0.94)	*(0.58)*	*(0.58)*
Manure	75	65	59
	(0.01)	*(0.01)*	*(0.01)*
Lime	13,041	7,277	9600
	(0.67)	*(0.38)*	*(0.34)*
Pesticide	8,200	4365	7534
	(0.40)	*(0.16)*	*(0.24)*
Electricity	10,660	12,500	13618
	(0.54)	*(0.44)*	*(0.51)*
Fixed cost			
Land use cost	40,290	42,014	39,627
	(1.68)	(1.46)	(1.36)
Interest on Operating Cost	94,373	1,05,725	1,22,252
	(4.68)	(4.69)	(4.70)
Total	**19,63,124**	**23,63,965**	**26,30,459**
	(200)	(200)	(200)

Source: Author own compilation, 2025

From the above table, it is measure that the costing pattern is divided for two parts, fixed cost and variables cost. Most of the portion has covered by human-labor that varies from three categories of farmers. Marginal farmers spend most money for human labor purposes, and medium farmers' costs fewer below compared than marginal farmers. A big portion has been spent for feed-purchasing purchases for small and medium famers, which uplifts their costing pattern. The cost of fingerlings varies from farm size and fish quality, where marginal famers faces huge costing for fingerlings. The second portion denotes fixed cost, where land use and interest over operating cost are two parts, mostly marginal farmers bear most fixed cost as interest bearing factors.

Table 4: Multiple Regression Model to measure the Impact of Independent Variables

Variables Name	Variable Sign	Coefficient Value	t Value
Constant	2.698	1.890	0.872
Human labor cost (X_1)	0.214 **	0.097	2.201
Fingerlings cost (X_2)	0.009	0.105	0.086
Feed cost (X_3)	0.651 ***	0.149	9.987
Manure cost (X_4)	0.081 *	0.040	1.775
Fertilizer cost (X_5)	-0.056	0.082	-0.919
Lime cost (X_6)	0.079	0.049	1.674
Pesticide cost (X_7)	0.009	0.032	0.281
Water supply cost (X_8)	0.135 **	0.065	2.077
Electricity cost (X_9)	0.086	0.082	1.049
Environmental Knowledge (X_{10})	*0.045**	0.033	1.85
F-value (N = 60)	*27.20*		
R2	*0.94*		
Returns to scale	*1.72*		

Source: Author own compilation, 2025

4. DISCUSSION

From the above table, it is known that Labor Costing, Manure Costs, fish food, and water supply costs have a significant relation with fish production per hectare. If the human capital is more utilized for pond-processing, fish production will be increased will be increased significantly. Secondly, Feed cost has a positive connection with fish production, increasing feed cost helps to enhance fish production by nearly 65 per cent, which is statically significant at a 1 per cent level. Thirdly, manure cost has a positive connection with the production, when farmers start farming the waste of hen ducks is mixed with water, which is a natural source of protein and vitamins for fishes. Fourthly, water supply has a positive and significant connection with production, proper water supply leads to enhanced fish production per hectare. Fifthly, most farmers have no idea about environmentally friendly fish-feed supply, which is called green feed for fish, environmental knowledge is one of the emerging issues for fish production, it is highly connected with basic environmental knowledge which is depicted in Table no 2 in this research. When all over the world is trying to achieve sustainable goals by 2030, it is our core duty to establish the practice of eco fish-feed production and consumption. It is noticed that environmental knowledge also helps to ensure the growth of fish production per hectare. It is also statistically significant.

5. CONCLUSIONS

Sustainable fish production is one of the challenging issues for rural farmers, but fish marketing and supply are two well connected factors that help to ensure profit margin at the maximum level. In most cases, local fish farmers do not grab the fragrance of profit properly which it grabs by middlemen who control farmers and final consumers badly. By studying the fish marketing channel and their cost and profit margins some recommendations are drawn which are given below. Fish is a highly perishable product that needs proper preservation facilities for marketing. It is needed to move fish distance places for marketing. So transportation and shipment facilities should be improved. It is the basic requirement of the establishment of a sufficient ice factory adjacent to the cultural ground. It is necessary to introduce modern wholesaling and retailing facilities. To improve the hygienic conditions of landing centres and markets. Keep the constant price of fish by the government. Avoiding middlemen during fish marketing is a key factor in improving the market share of farmers. Local, National and International NGOs and also Government should provide technical knowledge and credit sources for the agents of fish marketing. Ensure better marketing and distribution of fish. With the increasing of middlemen, the market share of fishermen decreases and the consumer price increases. The result shows that there is a huge gap between the farmed price and the consumer-level price. This indicates the longer the marketing channel, the lesser the share of the fisherman and the higher the marketing margins. Alternatively, the shorter the marketing channel, the higher the share of the fisherman and the lower the marketing margins. To develop and improve the fish marketing channel, the unnecessary and exploitative middleman should be eliminated. In future, some research may be conducted with sustainable fish-farming and environmental knowledge where green economy and eco cultivation should be prioritized. So, government and public-private relationships are essential to improve the existing fish marketing system.

REFERENCES

Ahmed, N., & Rahman, M. M. (2004). A study on fish marketing system in Gazipur, Bangladesh. *Pakistan Journal of Biological Sciences, 8*(2), 287–292.

Ahmed, N., Zander, K. K., & Garnett, S. T. (2011). Socioeconomic aspects of rice-fish farming in Bangladesh: Opportunities, challenges and production efficiency. *Australian Journal of Agricultural and Resource Economics, 55*(2), 199–219.

Al-Amin, A. Q., Alam, G. M., & Hassan, C. H. (2012). Analysis of inshore economic benefit and growth through the proper uses of the utility and scope of fisheries and livestock: A guideline to the MOFL in Bangladesh. *Asian Journal of Animal and Veterinary, 7*, 477–488.

Bangladesh Economic Review. (2022, June). Economic Advisers Wing, Finance Division, Ministry of Finance.

Busari, A. O. (2018). Economic analysis of homestead fish farming in Olorunda local government area, Osun State, Nigeria. *Nigerian Journal of Fisheries and Aquaculture, 6*(2), 19–26.

Deb, A., Chandan, C. S. S., Roy, P., Hossain, M. I., & Bari, S. M. (2021). Inland aquaculture and fish health management: A case study of Sylhet district in Bangladesh. *Aquaculture Studies, 21*(3), 129–137.

Department of Fisheries (DoF). (2015). *Fishery statistical yearbook of Bangladesh*. Ministry of Fisheries and Livestock, Bangladesh.

Department of Fisheries (DoF). (2016). *National Fish Week Compendium* (In Bengali). Ministry of Fisheries and Livestock, Bangladesh.

Department of Fisheries (DoF). (2018). *Fishery statistical yearbook of Bangladesh*. Ministry of Fisheries and Livestock, Bangladesh.

Department of Fisheries (DoF). (2022). *Yearbook of fisheries statistics of Bangladesh, 2021–2022*. Fisheries Resources Survey System (FRSS), Ministry of Fisheries and Livestock, Bangladesh.

Ebukiba, S. E., & Anthony, L. (2019). Economic analysis of catfish production in Karu Local Government Area, Nassarawa State, Nigeria. *IOSR Journal of Agriculture and Veterinary Sciences, 12*(3), 41–48.

Eckstein, D., Kunzel, V., & Schafer, L. (2021). *Global climate risk index 2021* (pp. 10–15). Germanwatch. https://www.germanwatch.org/en/cri

Ele, E. I., Out, I., Obong, E. A., Iniobong, O., Okon, E., & Udoh, E. (2013). Economic analysis of fish farming in Calabar, Cross River State, Nigeria. *Greener Journal of Agricultural Sciences, 3*, 542–549.

El-Naggar, G. O., Nasr-allah, A. M., & Rasaki, K. (2008). Economic analysis of fish farming in Behera Governorate of Egypt. *International Symposium on Tilapia in Aquaculture, 10*, 4794–4803.

Food and Agriculture Organization (FAO). (2012). *The state of world fisheries and aquaculture 2012*. FAO Fisheries and Aquaculture Department.

FAO. (2013). *Software for fishery and aquaculture statistical time series*. http://www.fao.org/fishery/statistics/software/fishstatj/en

FAO. (2016). *Food and agriculture—Key to achieving the 2030 agenda for sustainable development*.

FAO. (2020). *The state of world fisheries and aquaculture 2020: Sustainability in action*. https://doi.org/10.4060/ca9229en

FAOSTAT. (2016). *Statistical database*. Food and Agriculture Organization of the United Nations.

Faruk, M. A. R. (2003). *A comparative economic analysis of carp and pangus culture in some selected areas of Mymensingh district* (Unpublished master's thesis). Bangladesh Agricultural University, Mymensingh.

Ferdoushi, Z., Patwary, Z. P., Ara, Y., & Rana, M. (2019). Economic analysis of tilapia farming in some selected areas of Dinajpur District: A comparison between monoculture and polyculture. *Journal of Bangladesh Agricultural University, 17*(1), 117–121.

Ghose, B. (2017). *Fisheries and aquaculture in Bangladesh: Challenges and opportunities*.

Hasan, J., Lima, R. A., & Shaha, D. C. (2021). Fisheries resources of Bangladesh: A review. *International Journal of Fisheries and Aquatic Studies, 9*, 131–138. https://doi.org/10.22271/fish.2021.v9.i4b.2532

Hasan, M. R., & Ahmed, G. U. (2002). Issues in carp hatcheries and nurseries in Bangladesh, with special reference to health management. *FAO Fisheries Technical Paper, 406*, 147–164.

Islam, M. M., Barman, A., Kundu, G. K., Kabir, M. A., & Paul, B. (2019). Vulnerability of inland and coastal aquaculture to climate change: Evidence from a developing country. *Aquaculture and Fisheries, 4*(5), 183–189. https://doi.org/10.1016/j.aaf.2019.02.007

Islam, M. R., Haque, M. M., & Rahman, M. M. (2017). Strength and weakness of existing traceability system of seafood production in Bangladesh. *Program of Agriculture, 28*, 160–162.

Islam, M. S., Murshed, S. M. M., Moniruzzaman, M., & Baree, M. A. (2002). Rice-cum fish farming in selected areas of Mymensingh district. *Online Journal of Biological Sciences, 2*, 715–718.

Islam, N., Haque, E., & Mohsin, A. B. M. (2008). Carp culture: Cost-return and profit analysis of Rajshahi district. *Bangladesh Journal of Fisheries, 3*(3), 52–55.

Itam, K. O., Etuk, E. A., & Ukpong, I. G. (2014). Analysis of resource use efficiency among small-scale fish farms in Cross River State, Nigeria. *International Journal of Fisheries and Aquaculture, 6*(7), 80–86.

Kumar, B., Sharma, R., Lakra, W. S., Sharma, A., Prakesh, S., & Sharma, M. M. (2022). Economic assessment of shrimp farming (*Litopenaeus vannamei*) in Gujarat—A profitable venture. *International Journal of Innovative Research in Science Engineering and Technology, 5*(8), 15334–15342.

Manik, M. H. (2023). Movement of the economy of Bangladesh with its sector-wise contribution and growth rate. *Journal of Production, Operations Management and Economics, 3*(2), 1–8. https://doi.org/10.55529/jpome.32.1.8

Mazid, M. A. (2002). *Development of fisheries in Bangladesh: Plan and strategies for income generation and poverty alleviation*. Dhaka: Nasima Mazid.

Mondal, G. (2008). *Effects of land use changes on livelihood pattern of small farmers*.

Sarker, F. C., Rahman, M. K., Sadat, M. A., Shahriar, A., & Nowsad Alam, A. K. M. (2022). Haor-based floodplain-rich freshwater ichthyofauna in Sylhet Division, Bangladesh: Species availability, diversity, and conservation perspectives. *2*(4), 639–661.

Shamsuzzaman, M. M., Islam, M. M., Tania, N. J., Al-Mamun, M. A., Barman, P. P., & Xu, X. (2017). Fisheries resources of Bangladesh: Present status and future direction. *Aquaculture and Fisheries, 2*(4), 145–156.

Shawon, N. A. A., Prodhan, M. M. H., Khan, M. A., & Mitra, S. (2018). Financial profitability of small-scale shrimp farming in a coastal area of Bangladesh. *Journal of Bangladesh Agricultural University, 16*(1), 104–110.

Singha, C., & Chandan, S. (2023). Aquaculture practices in Bangladesh: A synopsis on prospects, productivity and problems. *December*. https://doi.org/10.1111/jwas.13045

Sunny, A. R., Mithun, M. H., Prodhan, S. H., Ashrafuzzaman, M., Rahman, S. M. A., Billah, M. M., & Hossain, M. (2021). Fisheries in the context of attaining sustainable development goals (SDGs) in Bangladesh: COVID-19 impacts and future prospects. *Sustainability, 13*(17), 9912. https://doi.org/10.3390/su13179912

Tamim, A. T., Begum, H., Shachcho, S. A., Khan, M. M., Yeboah-Akowuah, B., Masud, M., & Al-Amri, J. F. (2022). Development of IoT based fish monitoring system for aquaculture. *Intelligent Automation & Soft Computing, 32*(1).

.

CLIMATE CHANGE AS A THREAT MULTIPLIER: ASSESSING ITS IMPACT ON RESOURCE SCARCITY, MIGRATION, AND POLITICAL INSTABILITY

Igor Britchenko
University of the National Education Commission
Krakow, Poland
https://orcid.org/0000-0002-9196-8740
igor_britchenko@pltch-sci.com

Abstract. *This article examines the conceptualization and application of climate change as a "threat multiplier" in global security discourse. Originating within the U.S. national security community, the term describes how the physical impacts of climate change interact with and exacerbate pre-existing social, economic, and political vulnerabilities, thereby multiplying threats to peace and stability. While the framework has been instrumental in placing climate change on the security agenda, it is also critiqued for potentially constraining policy responses to a reactive, management-oriented posture rather than promoting transformative change. This study employs a qualitative, comparative case study methodology to deconstruct the threat multiplier effect through its cascading impacts. It first analyzes the first-order impact of climate change on critical resources, with a focus on water stress in the Middle East and North Africa (MENA) and food insecurity in Sub-Saharan Africa and South Asia. It then investigates the second-order human consequence of climate-induced migration, examining patterns in the Sahel, Bangladesh, and Central America, and highlighting the profound legal and geopolitical challenges posed by the lack of international protection for "climate refugees." Finally, through in-depth case studies of Syria and Sudan, the article analyzes how these combined pressures can culminate in the third-order outcome of political instability and violent conflict. The analysis reveals that governance is the critical mediating variable determining whether climate stress leads to instability. The article concludes by assessing the policy responses of the United Nations, European Union, and the United States, identifying key gaps, and advocating for an integrated policy framework that merges climate adaptation, development, and peacebuilding to address the multifaceted nature of climate-related security risks.*

Keywords: Climate Change; Threat Multiplier; Resource Scarcity; Water Stress; Food Insecurity

1. INTRODUCTION

The discourse surrounding climate change has evolved significantly over the past two decades, moving from a predominantly environmental issue to a central concern of international peace and security. This shift has been catalyzed by the widespread adoption of a powerful, albeit contested, conceptual framework: climate change as a "threat multiplier." This introduction traces the origins and diffusion of this concept, establishes the critical debate surrounding its utility and implications, and outlines the objectives of this article, which seeks to systematically unpack the complex causal pathways through which climate change destabilizes vulnerable regions.

1.1. DEFINING THE "THREAT MULTIPLIER": A CONCEPT'S JOURNEY FROM A MILITARY TO A GLOBAL STAGE

The term "threat multiplier" was strategically coined in 2007 by the CNA (Center for Naval Analyses) Military Advisory Board, a group of retired U.S. generals and admirals led by Sherri Goodman (CNA Military Advisory Board, 2007; Goodman, 2023). The term was a deliberate and astute play on the familiar military concept of a "force multiplier," designed to frame the security implications of climate change in a language that would resonate deeply within the defense and national security communities (Goodman, 2023). Its core analytical function is to articulate how the physical phenomena of a warming world—such as rising global temperatures, changing precipitation patterns, and climbing sea levels—do not create security threats in a vacuum. Instead, they interact with and exacerbate a wide array of pre-existing vulnerabilities and drivers of instability, including poverty, infectious disease, terrorism, and weak governance (CNA Military Advisory Board, 2007; Hagel, 2014). This framing intentionally avoids the pitfalls of simplistic environmental determinism by emphasizing complex interaction and amplification rather than direct, linear causation (Busby, 2018).

The concept proved remarkably effective. It was rapidly adopted as the "primary lens" through which the U.S. national security community began to make sense of climate change (Dalby, 2024). It appeared in high-level speeches by officials like Secretary of Defense Chuck Hagel and was integrated into foundational documents such as the U.S. National Security Strategy and Department of Defense (DoD) adaptation roadmaps (Hagel, 2014; The White House, 2022). This framing allowed security analysts to aggregate a diverse set of climate impacts—from water and food shortages to increased demand for humanitarian assistance and the degradation of military coastal installations—into a coherent and pressing national security problem (Dalby, 2024). From this influential American context, the "threat multiplier" framing subsequently "jumped... to a global setting," permeating the discourse of international organizations like the United Nations (UN) and the European Union (EU), where it continues to shape policy and analysis (Dalby, 2024; European Union, 2008; Brown & McLeman, 2009).

1.2. A CONTESTED FRAMEWORK: "THREAT MULTIPLIER" AS A "DISMAL WORLDMAKING PROJECT"

Despite its widespread adoption, the "threat multiplier" framework is the subject of significant academic and policy critique. Some scholars argue that its ascendance represents a "dismal and limited worldmaking project" that, while successful in gaining attention, ultimately constrains effective action more than it enables it (Dalby, 2024). The critique posits that the framework is "dismal" because it fosters a pessimistic, mechanistic, and almost fatalistic view of the future—one of inevitable climate-intensified conflict, humanitarian disaster, and instability, particularly located in the fragile states of the Global South (Dalby, 2024; Read, 2021).

Furthermore, the framework is seen as "limited" because it channels responses toward incrementalist management of symptoms rather than promoting the transformative change—namely, rapid and systemic decarbonization—required to address the root cause of climate insecurity (Dalby, 2024). By framing climate change as a security threat, it aligns the problem with the existing bureaucratic mandates and operational modes of defense, intelligence, and security agencies. These institutions are inherently geared toward threat management, risk mitigation, and reactive response, such as hardening military infrastructure against sea-level rise or conducting climate-themed wargames (Dalby, 2024). This focus on adaptation within the security sector, while necessary, risks diverting attention and resources from the more fundamental, albeit more politically difficult, task of emissions reduction. This has led some analysts to argue that the framing is now outdated and that climate change should be viewed not as a mere multiplier but as the "main threat" or a "hyperthreat" in its own right, a challenge so foundational that it requires an entirely new strategic paradigm (PLAN E, 2022).

The very success of the "threat multiplier" concept has thus created a profound policy paradox. The term was a powerful tool for agenda-setting, successfully convincing a security-focused audience that might otherwise have dismissed environmental concerns to take the issue seriously (Goodman, 2023). Yet, in doing so, it may have inadvertently locked the problem into a conceptual and institutional box that is ill-suited to delivering the most effective and holistic solutions. The framework can also carry a subtle geopolitical bias. Originating in the U.S. security community, its application often focuses on threats *emanating from* the Global South—instability in Africa, migration from Central America—that could impact the security interests of the Global North (Dalby, 2024; Koubi, 2019). This can externalize the problem, portraying vulnerable regions as sources of future threats to be managed or contained, rather than as the primary victims of a global crisis disproportionately caused by the historical emissions of industrialized nations. These dynamic risks prioritizing containment strategies, such as enhanced border security, over justice-oriented solutions like robust climate finance and technology transfer.

1.3. RESEARCH PROBLEM AND OBJECTIVES

The central research problem animating this article is the critical gap between the widespread political and institutional use of the "threat multiplier" concept and a nuanced, empirically grounded understanding of the specific causal pathways through which it operates. As critics have noted, the phrase itself "doesn't tell you much about what combination of factors we should be worried about" (Busby, 2018). It serves as a powerful but vague shorthand.

Therefore, this article aims to deconstruct the "threat multiplier" effect by tracing its cascading impacts through a multi-layered analysis. The objectives of this study are:

1. To review the theoretical foundations of the climate-security nexus, establishing a robust analytical framework for the study.
2. To systematically analyze the first-order impact of climate change on the degradation of critical natural resources, specifically water, food, and arable land.
3. To examine the second-order human consequence of this resource stress: climate-induced migration and displacement, and the associated legal and geopolitical challenges.
4. To investigate, through specific and detailed case studies, how these compounding pressures can cascade into the third-order outcome of political instability and violent conflict.
5. To critically assess major international and national policy responses to these challenges and provide evidence-based recommendations for a more integrated and effective climate-security architecture.

By pursuing these objectives, this article seeks to move beyond the slogan of "threat multiplier" to provide a detailed, evidence-based account of the mechanisms that link a changing climate to a more fragile and contentious world.

2. THEORETICAL FOUNDATIONS OF THE CLIMATE-SECURITY NEXUS

To properly analyze how climate change multiplies threats, it is essential to ground the inquiry in established theoretical frameworks. The concept is situated at the intersection of two evolving fields of study: environmental security and the climate-conflict nexus. This section reviews the key concepts from this literature, explains the analytical model that informs this paper, and highlights why a qualitative, process-tracing approach is vital for understanding these complex, context-dependent phenomena.

2.1. ENVIRONMENTAL SECURITY: FROM COLD WAR TO ANTHROPOCENE

The field of environmental security emerged from the environmental movements of the 1970s and gained significant academic and policy traction following the end of the Cold War (Read, 2021). Its core intellectual contribution was to broaden the traditional, state-centric, and military-focused definition of "security" to include non-military threats, such as environmental degradation (Read, 2021; Barnett, 2007). Early research, notably from the Toronto Group, sought to establish empirical, causal connections between environmental scarcity and violent conflict (Homer-Dixon, 1994). While influential, this initial wave of research was later criticized for sometimes overstating direct causality and for a disproportionate focus on the Global South, a critique that remains relevant to the "threat multiplier" discourse today (Read, 2021).

A pivotal evolution in the field was the integration of "human security," which shifts the referent object of security from the state to the well-being of individuals and communities (Read, 2021; UNDP, 1994). This perspective is indispensable for analyzing climate change, whose impacts are ultimately experienced at the human level through threats to livelihoods, health, food, and physical safety (Read, 2021). This paper adopts a definition that synthesizes these state- and human-centric views, defining environmental security as the "ability of individuals, groups, or states to adapt to, mitigate, or avoid environmental change without critical adverse effects" that degrade their well-being and integrity (Read, 2021). Climate change thus represents the most profound challenge to environmental security in the Anthropocene.

2.2. THE CLIMATE-CONFLICT NEXUS: PATHWAYS AND MEDIATING FACTORS

The academic literature examining the direct link between climate change and violent conflict is characterized by vigorous debate and a lack of broad consensus on causality (Koubi, 2019; Selby et al., 2017). Most researchers now agree that the relationship is not one of direct cause-and-effect but is complex, indirect, and highly contingent on context (Koubi, 2019; Theisen et al., 2013; Detges, 2017). Instead of climate change directly causing war, it creates or exacerbates conditions that can increase the risk of conflict.

Recent literature reviews have converged on four primary, indirect causal pathways that link climate variability to violent conflict (Koubi et al., 2024):

1. Economic Shocks: Climate-related disasters or agricultural losses can depress economic activity. This reduces the opportunity cost of violence, making recruitment into armed groups a more attractive option for individuals with diminished livelihood prospects.
2. Agricultural Decline: The failure of crops and the erosion of food security can fuel widespread grievances against the state, undermine livelihoods, and lead to food riots or social unrest.
3. Natural Resource Competition: Increasing scarcity of essential resources, particularly water and arable land, can intensify competition and conflict between different livelihood groups, such as farmers and pastoralists.
4. Migration and Displacement: Climate-induced population movements can place new pressures on resources in receiving areas and, in some contexts, stoke social and ethnic tensions between migrant and host communities.

Crucially, the activation of these pathways is not automatic. Whether climate stress translates into violent conflict is mediated by a host of powerful contextual factors. The evidence consistently shows that the most important determinants are not the climatic variables themselves, but the underlying social and political conditions of the society they affect. These mediating factors include the quality of governance and institutional capacity to manage resources and resolve disputes; pre-existing socio-economic conditions like poverty, inequality, and dependence on climate-sensitive livelihoods; and political factors such as the political exclusion of certain groups, elite competition, and a history of inter-group tensions (Busby, 2018; Koubi, 2019; Mobjörk et al., 2020). This leads to a foundational conclusion: a society's vulnerability to climate-related conflict is more a function of its political and social resilience than its geographic exposure to climate change. Consequently, the most effective "climate security" policies may not be climate-centric at all, but rather those that focus on building good governance, inclusive economic development, and robust conflict resolution mechanisms.

2.3. ANALYTICAL APPROACH: BEYOND STATISTICAL CORRELATION

Given the complexity and context-dependency of the climate-security nexus, this article employs a qualitative, comparative case study methodology. While quantitative studies are invaluable for identifying broad correlations, they often struggle to capture the intricate, non-linear processes that connect a climate shock to a political outcome (Selby et al., 2017; van Baalen & Mobjörk, 2018). Statistical models using fixed-effects, for example, can isolate a climatic effect on conflict risk but, by design, control for the very socio-political variables that explain the causal mechanism, leading to a situation where a model "actually tells us little" about the broader story of conflict (O'Loughlin et al., 2014).

More advanced methods like Structural Equation Modeling (SEM) and machine learning are beginning to quantify both direct and indirect pathways with greater sophistication (Koubi et al., 2022; Gao et al., 2022). However, a qualitative approach is uniquely suited to "process tracing"—that is, examining the sequence of events and the specific social, economic, and political mechanisms that link climate stressors to instability in a particular case. By systematically examining a diverse set of cases where climate has been implicated as a threat multiplier (e.g., Syria, Sudan, the Sahel), this study can identify common causal patterns as well as critical differences, providing a richer, more textured understanding than a purely quantitative analysis could offer alone.

This analytical approach is further informed by an emerging frontier in climate research: coupled social-climate models. Traditional models often treat the relationship as a one-way street: human socio-economic systems impact the climate (Menard et al., 2021). However, this misses the crucial feedback loop whereby climate impacts—such as extreme weather events or resource scarcity—in turn alter human behavior, social norms, and political dynamics (Menard et al., 2021). New models, often employing tools like evolutionary game theory, are being developed to capture these two-way feedbacks (Menard et al., 2021; Kahl, 2006). A key finding from this work is that social factors, such as high levels of economic inequality or social fragmentation (homophily), can themselves significantly worsen climate outcomes by hindering collective action on mitigation, leading to a higher peak temperature anomaly (Menard et al., 2021). This reinforces the central argument that social and political dynamics are not merely *outcomes* of climate change; they are fundamental *drivers* of the climate future, making social and political resilience a prerequisite for environmental stability.

3. THE FIRST-ORDER IMPACT: CLIMATE-INDUCED RESOURCE SCARCITY

The "threat multiplier" effect begins with a direct, physical impact: the degradation of the natural resource base upon which human societies depend for survival and prosperity. Climate change, through its influence on temperature and the hydrological cycle, is systematically intensifying the scarcity of water, food, and arable land in many of the world's most vulnerable regions. This section provides the empirical foundation for the subsequent analysis of migration and instability by detailing these first-order impacts, using regional case studies to illustrate their scale and severity.

3.1. WATER STRESS AND DESERTIFICATION: THE DRYING OF VULNERABLE REGIONS

Climate change directly intensifies water stress through multiple mechanisms: decreased and more erratic precipitation, increased evaporation from soil and reservoirs due to higher temperatures, and altered runoff patterns from the accelerated melting of glaciers. The Intergovernmental Panel on Climate Change (IPCC) projects that drought conditions in parts of Asia could increase by 5-20% by the end of this century (IPCC, 2022). This physical stress is often compounded by human factors, creating a potent recipe for crisis.

- *Case Study: The Middle East and North Africa (MENA)*

The MENA region is the epicenter of global water scarcity, home to 12 of the world's 17 most water-stressed countries (World Bank, 2023). Despite having nearly 6% of the global population, the region has access to only 1% of the world's renewable freshwater resources (Sowers et al., 2011). Climate change is a primary driver of this crisis, with scientific models predicting a 10-20% decline in rainfall by mid-century

(Sowers et al., 2011). This climatic pressure is dangerously amplified by rapid population growth, accelerating urbanization, and profound inefficiencies in water use, particularly in the agricultural sector, which accounts for up to 85% of all freshwater withdrawals (Sowers et al., 2011). The economic consequences of inaction are dire; the World Bank projects that unchecked water stress could reduce the region's GDP by as much as 14% by 2050 (World Bank, 2023).

A critical dynamic observed across the region is a vicious cycle of maladaptation. In response to climate-induced surface water shortages, farmers and governments turn to the only available alternative: groundwater. This leads to the massive and unsustainable over-extraction of non-renewable fossil aquifers. In Syria before the war, government subsidies for water-intensive crops like cotton encouraged huge inefficiencies in irrigation and massive groundwater pumping (de Châtel, 2014). In Jordan, groundwater is currently being extracted at a rate three times faster than its natural recharge rate (Sowers et al., 2011). This short-term coping strategy is deeply maladaptive, transforming a recurring climate problem (drought) into a potentially permanent resource crisis (aquifer depletion), creating a more profound and irreversible form of scarcity for future generations.

- *Spotlight on Morocco:* This North African nation provides a clear example of these converging pressures. Morocco has experienced a 30% reduction in average rainfall over the past two decades, severely impacting its water reserves and agricultural sector (Sowers et al., 2011). Detailed hydrological studies of its major river basins, such as the Ziz and Souss, reveal a system under extreme stress from both climate change and surging agricultural demand (Bouchaou et al., 2024; Karmaoui et al., 2019). Projections indicate a likely future decrease in water supply of up to 27%, threatening the viability of its agricultural economy (Karmaoui et al., 2019). In response, Morocco is pursuing a national strategy focused on large-scale infrastructure projects, including major investments in seawater desalination and wastewater treatment and reuse, to augment its water supply (Chatham House, 2024).
- *Spotlight on Jordan:* Jordan stands as one of the most water-poor nations on earth, with per capita water availability far below the threshold of absolute scarcity (Sowers et al., 2011; World Bank, 2025). Climate change is projected to reduce the country's already meager water resources by a further 30% by 2040 (World Bank, 2025). This climatic stress is compounded by immense demographic pressure, including a population that has more than doubled in a decade, partly due to the influx of refugees from regional conflicts. The arrival of Syrian refugees alone caused Jordan's national water demand to spike by 20% in just five years (Sowers et al., 2011). The crisis has forced the government to implement strict water rationing, with many households in Amman receiving piped water for only 12-24 hours per week, and has driven a dangerous reliance on the unsustainable mining of groundwater (World Bank, 2025).

3.2. FOOD INSECURITY AND AGRICULTURAL COLLAPSE

Climate change poses a fundamental threat to global food security, affecting all its core dimensions: availability (the physical supply of food), access (the ability of people to afford and obtain food), and utilization (the nutritional value of food) (WFP, 2016; Sowers et al., 2011). The mechanisms are varied and include direct impacts on crop yields from heat and water stress, shifts in the geographic range of agricultural pests and diseases, and the long-term degradation of soil and arable land (WFP USA, 2021; Theisen et al., 2013). A general rule of thumb for the tropics is that for every 1°C of mean temperature rise, staple crop yields can be expected to decline by approximately 10% (WFP USA, 2021).

- *Case Study: Sub-Saharan Africa*

The region is exceptionally vulnerable to climate-induced food insecurity due to its high dependence on rain-fed agriculture, which is intrinsically sensitive to rainfall variability, and its generally low institutional and financial capacity to adapt (Teka et al., 2024; Van Baalen & Mobjörk, 2018). The Food and

Agriculture Organization (FAO) has projected that climate change could lead to yield losses of up to 50% for key staple crops like maize, sorghum, and millet by the year 2050, a catastrophic outcome for a region already struggling with malnutrition (FAO, 2025). This agricultural stress is compounded by widespread land degradation and desertification, which already affects 45% of Africa's land area, with up to 65% of its productive land considered degraded (UN News, 2021). The Sahel, an arid band stretching across the continent, is a particular hotspot for these converging crises (WFP USA, 2021). The International Monetary Fund (IMF) confirms that climate change is actively intensifying food insecurity across Sub-Saharan Africa, with a series of recent climate shocks helping to push the number of people suffering from high malnutrition to 123 million in 2022 (IMF, 2022).

- *Case Study: South Asia*

South Asia is another region where climate change poses a grave threat to food security, driven by its high population density, large agrarian population, and exposure to a range of climate hazards (South Asia Times, 2025; World Bank, 2023). The IPCC projects significant declines in crop production across the region as warming continues. In India, for example, rice production could fall by 10-30% and maize production by 25-70% under warming scenarios of 1°C to 4°C (IPCC, 2022). The impacts are not just projections; they are already occurring. The devastating floods in Pakistan in 2022 inundated 1.7 million hectares of prime agricultural land (South Asia Times, 2025). Severe heatwaves in India have damaged wheat crops, forcing the government to impose export restrictions to ensure domestic supply, with ripple effects on global markets (South Asia Times, 2025; Zittis et al., 2021). The World Food Programme (WFP) consistently identifies South Asia as a region of high concern, where climate vulnerability, poverty, and hunger are deeply intertwined (WFP USA, 2021; World Bank, 2021).

These resource crises are not merely environmental; they are powerful drivers of economic restructuring and inequality. The collapse of agricultural livelihoods in vulnerable regions forces a mass migration of labor from rural to urban areas, as seen in pre-war Syria (Peace Agency, 2021; de Châtel, 2014). This can create a glut of low-skilled labor in cities, depressing wages and straining public services, while simultaneously decimating the rural economic base. Wealthier actors, whether individuals or nations, may have the capacity to cope by securing remaining resources or importing food, while the poorest lose their land, livelihoods, and food security. The result is a fundamental reshaping of national economies and a widening of the gap between the climate-resilient and the climate-vulnerable, laying the social and economic groundwork for future instability.

4. THE HUMAN CONSEQUENCE: CLIMATE-INDUCED MIGRATION AND DISPLACEMENT

As climate change degrades the resource base upon which livelihoods depend, it triggers a profound second-order impact: the movement of people. Climate-induced migration and displacement represent one of the most significant human consequences of the environmental crisis. This section analyzes the complex patterns and drivers of this mobility, explores the immense legal and geopolitical challenges it creates, and illustrates these dynamics through regional case studies.

4.1. PATTERNS AND DRIVERS OF CLIMATE MOBILITY: A MULTI-CAUSAL PHENOMENON

Climate-related human mobility is a complex and multifaceted phenomenon, not a single, uniform event. It is essential to distinguish between displacement caused by sudden-onset disasters, such as floods and cyclones that force immediate and often large-scale but sometimes temporary evacuation, and migration driven by slow-onset processes like drought, desertification, and sea-level rise, which tend to produce more gradual and permanent population shifts (Mobjörk et al., 2020; Rigaud et al., 2018; Schipper, 2020).

Crucially, migration is rarely a decision driven by climate factors alone. Research consistently shows it to be a multi-causal process where climate change acts as a potent "threat multiplier" for a host of underlying economic, social, and political drivers (IOM, 2023; American Security Project, 2019). A family may decide to move after their harvest fails (an economic driver), but that harvest failure was made more likely by a climate-driven drought. Studies have shown, for instance, that households experiencing crop losses are significantly more likely to have a family member migrate (IIED, 2025).

In many parts of the world, particularly the Sahel, mobility has long been a traditional and vital coping strategy. Seasonal and circular migration allows pastoralist and agricultural communities to adapt to environmental variability, diversify their income, and reduce risk (World Bank, 2024; Red Cross, n.d.). However, when climate pressures intensify to the point where migration is no longer a choice but a desperate act of survival (distress migration), it can lead to significant financial, social, and cultural losses for those forced to move (Red Cross, n.d.). This highlights a critical and often overlooked aspect of the issue: "trapped populations." These are often the most vulnerable groups—the elderly, the disabled, the extremely poor—who lack the financial and social resources to move and are left behind to face ever-deteriorating conditions (Schipper, 2020; Red Cross, n.d.).

4.2. THE GEOPOLITICAL CHALLENGE: A LEGAL VOID FOR "CLIMATE REFUGEES"

One of the most significant global challenges posed by climate-induced migration is the absence of a coherent international legal framework for the protection of those who cross borders. The term "climate refugee" is widely used in popular discourse, but it has no legal basis in international law and is a term that key agencies like the UN High Commissioner for Refugees (UNHCR) and the International Organization for Migration (IOM) have contested, preferring terms like "persons displaced in the context of disasters and climate change" (Global Governance Forum, 2022; The Wave, 2025; UNHCR, 2021).

The cornerstone of international protection, the 1951 Refugee Convention, defines a refugee as someone fleeing a "well-founded fear of being persecuted" for reasons of race, religion, nationality, membership of a particular social group, or political opinion (European Parliament, 2021). It was designed in the aftermath of World War II to protect people from state persecution and does not extend to those fleeing environmental degradation or natural disasters (European Parliament, 2021; McAdam, as cited in The Wave, 2025). This creates a "clear void" or a "legal limbo" in the international protection regime, leaving people displaced across borders by climate change without a recognized status or a clear set of rights (Global Governance Forum, 2022; The Wave, 2025).

While some legal scholars and activists are exploring alternative pathways for protection, such as arguments based on the fundamental "right to life" under international human rights law (as was tested in the landmark Teitiota v. New Zealand case before the UN Human Rights Committee), there is currently no legally binding international treaty specifically designed to protect climate migrants (Global Governance Forum, 2022; The Wave, 2025). This lack of legal status is not a mere technicality; it has profound real-world consequences, preventing the development and implementation of a predictable, coherent international framework for assistance, burden-sharing, and durable solutions (European Parliament, 2021). This legal void is not a simple oversight but reflects a deep-seated political reluctance among states, particularly in the Global North, to expand protection obligations that could apply to potentially hundreds of millions of people (IIED, 2025; The Wave, 2025). Given this political reality, progress is more likely to emerge from a patchwork of regional agreements, bilateral labor arrangements, and the slow evolution of human rights jurisprudence rather than a single, all-encompassing global treaty.

4.3. REGIONAL CASE STUDIES IN CLIMATE DISPLACEMENT

The Sahel: In this vast, arid region, mobility is a way of life. Population movement is overwhelmingly internal and often follows circular patterns, representing a centuries-old adaptation strategy to seasonal climate variability (World Bank, 2024). However, the intensification of climate change—manifesting as prolonged droughts and accelerating desertification—is converging with rampant insecurity and conflict, transforming traditional mobility into forced displacement (Mobjörk et al., 2020; Mixed Migration Centre, 2025). Climate change intersects with economic distress, primarily channeling migration through economic pathways; for example, a pastoralist family might move in search of work after losing their herd to drought (World Bank, 2024).

Bangladesh: This low-lying, deltaic, and densely populated nation is often described as "ground zero" for climate displacement. The primary drivers are a combination of slow- and sudden-onset hazards: relentless coastal and riverbank erosion, sea-level rise that contaminates freshwater with salt, and increasingly frequent and intense tropical cyclones (Rigaud et al., 2018; Displacement Solutions, 2012). The World Bank has projected that, without significant global mitigation action, up to 19.9 million people in Bangladesh could become internal climate migrants by 2050 (IIED, 2025; World Bank, 2021). This mass internal movement, largely directed toward overcrowded urban slums in cities like Dhaka, is creating immense social pressure and new vulnerabilities (Displacement Solutions, 2012). Horrifyingly, recent research has exposed a direct link between this climate-driven distress migration and modern slavery, with one study finding that over 90% of internal migrants from climate-affected areas experienced at least one indicator of forced labor, such as debt bondage or withheld wages (IIED, 2025).

Central America's "Dry Corridor": Stretching across parts of Guatemala, Honduras, and El Salvador, the "Dry Corridor" is experiencing more frequent and intense droughts linked to climate change, which are devastating the subsistence agriculture that forms the backbone of the rural economy (American Security Project, 2019; Alianza MX, 2025). Here, climate change acts as a "hidden driver" of migration. The more visible push factors are food insecurity and extreme poverty, but these are direct consequences of the climatic stress on agriculture (American Security Project, 2019). This dynamic fuels migration flows north toward Mexico and the United States, creating significant regional instability and a major geopolitical and humanitarian challenge at the U.S. southern border (Alianza MX, 2025).

These cases reveal a crucial paradox of mobility: it is simultaneously a sign of resilience and a symptom of extreme vulnerability. The ability to move can be a proactive adaptation strategy. Yet, the inability to move can signal the deepest poverty, while forced, distress-driven migration can expose people to new and even greater risks than those they fled. This paradox demands a sophisticated policy response that focuses not just on managing or preventing movement, but on building in-situ resilience to expand people's choices, while also ensuring that when migration does occur, it is safe, orderly, and respects the fundamental rights of those on the move.

5. THE ULTIMATE THREAT: POLITICAL INSTABILITY AND CONFLICT

This section represents the culmination of the cascading impacts analyzed thus far. It examines how the first-order pressures of resource scarcity and the second-order consequences of mass displacement, when filtered through contexts of poor governance, pre-existing grievances, and social fragility, can escalate into the third-order outcome of political instability and violent conflict. This is the final and most dangerous manifestation of climate change as a threat multiplier.

5.1. FROM ENVIRONMENTAL STRESS TO SOCIAL UNREST: THE TIPPING POINT

The causal pathways from environmental stress to violent conflict are consistently shown to be indirect and context-dependent. Climate change does not in itself cause wars; rather, it acts as a powerful amplifier, exacerbating the known drivers of instability and pushing fragile societies closer to a tipping point (Koubi, 2019; von Uexkull & Buhaug, 2021). Several key mechanisms facilitate this escalation:

- *Erosion of State Legitimacy*: When a government is perceived as unable or unwilling to respond effectively to climate-related disasters, provide relief, or manage scarce resources equitably, it can suffer a catastrophic loss of legitimacy. This failure fuels popular grievances and can create a fertile environment for anti-government protests and rebellion (de Châtel, 2014; von Uexkull & Buhaug, 2021).

- *Intensified Communal Competition*: The scarcity of vital resources like water and arable land can pit different livelihood groups against one another, most classically nomadic pastoralists against sedentary farmers. As climate change shrinks the available resource pie, traditional norms and mechanisms for sharing and dispute resolution can break down, leading to increased friction and violent communal conflict (Mobjörk et al., 2020; Carnegie Endowment, 2024; de Soysa & Rustad, 2010).
- *Exploitation by Non-State Armed Groups*: In regions with weak state presence, armed groups, insurgents, or terrorist organizations can exploit the chaos and desperation created by climate shocks. They can seize control of scarce resources (like water wells or fertile land) to fund their operations, or they can step into the governance vacuum, providing aid and services that the state cannot, as a means of winning support and recruiting fighters from desperate populations (Carnegie Endowment, 2024; Femia & Werrell, 2012).
- *Urban Instability*: The mass migration of people displaced from rural areas can overwhelm the infrastructure, housing, and job markets of cities. The growth of large, underserved slum populations on urban peripheries can create hotspots of social tension, crime, and political unrest, as seen in the lead-up to the Syrian civil war (Peace Agency, 2021; de Châtel, 2014).

5.2. CASE STUDY: SYRIA - DROUGHT AS A CATALYST FOR CIVIL WAR

The Syrian civil war is a canonical, though complex and contested, case study of the threat multiplier effect in action (Selby et al., 2017). The country experienced a historic and devastating drought between 2006 and 2010, an event that scientific research indicates was made significantly more likely and severe by anthropogenic climate change (Kelley et al., 2015; de Châtel, 2014; Gleick, 2014).

However, the drought's impact was catastrophically amplified by decades of the Assad regime's gross mismanagement of natural resources. Unsustainable agricultural policies, including massive government subsidies for water-intensive crops like wheat and cotton, had encouraged inefficient irrigation techniques and led to the severe depletion of the country's groundwater aquifers long before the drought began (de Châtel, 2014; Femia & Werrell, 2012). When the drought hit this pre-stressed system, the result was a complete collapse of agriculture and pastoralism in the country's northeast breadbasket. An estimated 75% of farming families suffered total crop failure, and herders lost up to 85% of their livestock (de Châtel, 2014).

This economic and social devastation triggered one of the largest internal displacements in recent history prior to the war, with up to 1.5 million people—mostly impoverished farmers and their families—forced to migrate from the countryside to the peripheries of already strained cities like Damascus, Homs, Aleppo, and Dara'a (Femia & Werrell, 2012; Kelley et al., 2015). The government's response to this massive humanitarian crisis was not one of assistance but of indifference and, eventually, repression. The state failed to provide relief, cut remaining subsidies which caused fuel prices to skyrocket, and ignored the simmering discontent (de Châtel, 2014). It was in the drought-stricken rural town of Dara'a that the initial protests of the Arab Spring in Syria erupted in March 2011. The protests, which initially followed the geographic path of the drought's impact, were met with brutal force, escalating a movement born of desperation and grievance into a full-blown, catastrophic civil war (de Châtel, 2014).

5.3. CASE STUDY: SUDAN - CLIMATE, RESOURCES, AND ENDURING CONFLICT

Sudan, and particularly its western region of Darfur, provides another stark example of how climate stress can interact with political and ethnic fault lines to fuel protracted conflict (Plowman, 2011). The region has experienced long-term climatic shifts toward greater aridity, punctuated by severe droughts in the 1970s and 1980s. This long-term desertification squeezed the available land and water resources, dramatically intensifying competition between the region's main livelihood groups: traditionally nomadic Arab pastoralist tribes and sedentary non-Arab farming communities (de Soysa & Rustad, 2010).

As in Syria, this environmental stress did not cause the conflict in isolation. Its explosive potential was unlocked by political factors. The conflict was mediated by the breakdown of the traditional tribal administrative systems that had historically managed resource disputes. Crucially, the central government in Khartoum did not act as an impartial arbiter. Instead, to suppress a rebellion by non-Arab groups, it pursued a strategy of arming and supporting local Arab militias, which became known as the Janjaweed, effectively taking sides in the resource conflicts and transforming them into a militarized, ethnicized, and politically charged civil war (de Soysa & Rustad, 2010).

The new conflict that erupted in Sudan in 2023 is creating a new "perfect storm." The widespread violence is severely disrupting agricultural seasons, blocking the migratory routes of pastoralists, and destroying livelihoods, all while the country continues to reel from the underlying pressures of climate change. This is creating a devastating feedback loop where conflict exacerbates environmental degradation and resource scarcity, which in turn fuels more conflict, pushing millions toward famine and creating an environment where armed groups can thrive (Carnegie Endowment, 2024).

These cases powerfully illustrate that governance is the master variable. In both Syria and Sudan, the decisive factor that turned environmental stress into mass violence was not the drought itself, but the nature of the state. A predatory, incompetent, or biased government that mismanages resources, fails to provide relief, and instrumentalizes ethnic tensions for political gain is the ultimate threat multiplier. Furthermore, climate change is actively reshaping the geography of conflict. In the Sahel, desertification is pushing pastoralists south into farmers' lands, creating an expanding zone of friction (Mobjörk et al., 2020). In Syria, displacement shifted the locus of unrest from rural areas to urban centers (de Châtel, 2014). In the Arctic, melting ice is creating an entirely new theater for great power competition (Hagel, 2014; Dalby, 2024). Security analysis must therefore become dynamic, anticipating how these environmental shifts will create new friction points and drive conflict into new domains.

Table 1: Comparative Analysis of Climate-Conflict Pathways in Case Studies

Feature	**Syria**	**Sudan (Darfur)**	**The Sahel**
Primary Climate Stressor	Severe multi-year drought (2006-2010), intensified by long-term warming and drying trend.	Long-term aridification and desertification, punctuated by severe droughts (1970s-80s).	Accelerating desertification, rainfall variability, and prolonged droughts.
Key Mediating Factors	Predatory and authoritarian governance; decades of water resource mismanagement; pre-existing social grievances.	Breakdown of traditional conflict resolution mechanisms; central government's ethnic favoritism and militarization of local disputes.	Weak state presence and porous borders; widespread poverty; pre-existing farmer-herder tensions.
Primary Impact Channel	Catastrophic agricultural collapse leading to mass internal migration from rural to urban areas.	Intensified competition for scarce water and grazing land between pastoralist and farming groups.	Livelihood erosion, distress migration as a coping strategy, and resource competition along shifting ecological zones.
Manifestation of Instability	Mass urban unrest in response to government inaction and repression, escalating into a full-scale civil war.	Large-scale, militarized communal violence and insurgency, characterized by ethnic cleansing and mass displacement.	Escalation of localized farmer-herder conflicts; exploitation of instability by extremist and criminal groups.

6. POLICY RESPONSES AND GLOBAL SECURITY IMPLICATIONS

The recognition of climate change as a security threat has prompted a range of policy responses from key international actors. These strategies, while varied in their institutional implementation, show a remarkable convergence in their conceptual approach. However, a significant gap persists between the stated goals of integrated, preventive action and the often-siloed, reactive reality of implementation. This section evaluates the current policy landscape, identifies critical shortcomings, and provides recommendations for a more robust and effective global climate-security architecture.

6.1. MULTILATERAL AND REGIONAL STRATEGIES: A PATCHWORK OF RESPONSES

The United Nations: The UN's primary institutional hub for this issue is the Climate Security Mechanism (CSM), established in 2018 as a joint initiative of the Department of Political and Peacebuilding Affairs (DPPA), the UN Development Programme (UNDP), the UN Environment Programme (UNEP), and the Department of Peace Operations (DPO) (UN CSM, 2022; UNSSC, 2021). The CSM's core mandate is to strengthen the capacity of the entire UN system to better analyze and address climate-related security risks. It does this by providing direct support to UN field missions, assisting with integrated risk assessments, developing analytical tools, and fostering a UN-wide community of practice to share knowledge and best practices (UN CSM, 2022; UNFCCC, n.d.). Reflecting this mainstreaming effort, the UN Security Council has increasingly recognized the adverse effects of climate change on stability in its resolutions and mission mandates for contexts such as Mali, Somalia, Iraq, and Sudan (UNSSC, 2021).

The European Union: The EU has formally adopted the "threat multiplier" framing and made the climate-security nexus a central pillar of its foreign and security policy (Brown & McLeman, 2009). The 2023 Joint Communication on a new outlook on the climate and security nexus outlines a comprehensive strategy to integrate climate considerations across all areas of EU external action, from diplomacy and development to defense and humanitarian aid (European Union, 2023; Copernicus SESA, n.d.). Operationally, this involves leveraging the EU's unique assets, such as the Copernicus Earth Observation program, to provide data and analysis for early warning of potential climate-related instability, such as food shortages or resource competition. This information is intended to inform diplomatic engagement and the planning of Common Security and Defence Policy (CSDP) missions and operations (Brown & McLeman, 2009).

The United States: The U.S. has had a fluctuating history of acknowledging climate change in its top-level strategic documents, with attention varying significantly between presidential administrations (American Security Project, 2019). The current approach, articulated in the 2022 National Security Strategy, identifies climate change as the "greatest and potentially existential" shared problem facing humanity (The White House, 2022). The U.S. Framework for Climate Resilience and Security provides a whole-of-government strategy organized around three core pillars: (1) Assess the potential impacts of climate-related threats through better data and analysis; (2) Partner with allies and vulnerable nations for an integrated approach; and (3) Invest in collective resilience, particularly in fragile states (U.S. Framework for Climate Resilience and Security, 2024).

A striking feature of these policy frameworks is their conceptual convergence. Despite different institutional arrangements, the UN, EU, and US have all independently arrived at a similar diagnosis and a similar prescription. They recognize that the problem is complex, interconnected, and context-specific, and they agree that the solution requires better evidence-based risk assessment, the breaking down of institutional silos, and deep partnerships with allies and affected communities. This emerging de facto consensus provides a solid foundation for enhanced international cooperation on climate security.

Table 2: Comparison of International Climate Security Frameworks

Feature	United Nations	European Union	United States
Core Conceptual Framing	Climate-related security risks	Climate change as a "threat multiplier"	Climate resilience and security
Primary Institutional Mechanism	Climate Security Mechanism (CSM) (DPPA, UNDP, UNEP, DPO)	European External Action Service (EEAS) & CSDP Missions	Interagency Framework (NSC, DoD, State, USAID, etc.)
Key Tools/Activities	Integrated risk assessments, support to field missions, capacity building	Earth Observation (Copernicus), diplomatic engagement, CSDP planning	Strategic dialogues, intelligence analysis, President's Emergency Plan for Adaptation and Resilience (PREPARE)
Stated Priority/Goal	Mainstream analysis across the UN system and support integrated responses	Enhance EU security and defense by tackling climate-driven instability	Strengthen the stability of nations and the resilience of communities, at home and abroad

6.2. IDENTIFIED GAPS AND RECOMMENDATIONS FOR INTEGRATED POLICY

Despite this policy convergence, significant gaps remain that hinder effective action on the ground. There is a fundamental tension between the stated goal of prevention in these strategies and the predominantly reactive nature of the security institutions often tasked with leading them. Policy documents are replete with calls for foresight, early warning, and upstream action to "break cycles of crisis" (U.S. Framework for Climate Resilience and Security, 2024). However, the core competencies and bureaucratic incentives of defense and security establishments are geared toward responding to crises once they erupt, not conducting the long-term, complex development work needed to prevent them. It is institutionally easier to secure funding to harden a military base against flooding (a reactive, tangible task) than it is to fund a decade-long agricultural resilience program in a fragile state (a preventive, but more complex and less visible task). This creates a persistent implementation gap between preventive rhetoric and reactive reality.

To bridge these gaps, this analysis identifies three critical areas for improvement and offers corresponding recommendations:

- *Gap 1: The Research-Policy-Practice Disconnect.* A chasm often exists between the nuanced findings of academic research, the formulation of high-level policy, and the realities of on-the-ground implementation. Peacebuilding scholarship, for instance, frequently overlooks climate drivers, while climate security analysis often neglects the principles and practices of peacebuilding. This can lead to missed opportunities for synergy (Eklöw & Mobjörk, 2024).
    - *Recommendation 1: Mandate Integrated Climate-Security Risk Assessments***.** To close this gap, integrated risk assessments that analyze the interplay of climate, conflict, and social vulnerability must become a mandatory, foundational step for all conflict analysis, peacebuilding planning, and development and humanitarian programming in fragile and climate-vulnerable regions (Eklöw & Mobjörk, 2024).
- *Gap 2: The Siloed Nature of Responses***.** Despite the rhetoric of integration, interventions often remain confined to institutional silos. Climate finance mechanisms are not always designed to be conflict-sensitive, and peacebuilding programs are not always climate-proofed (Eklöw & Mobjörk, 2024). This can lead to the dangerous phenomenon of "maladaptation," where well-intentioned climate adaptation projects—such as building a new dam or irrigation system—can inadvertently create new

resource conflicts or exacerbate existing social tensions if they are not designed with a deep understanding of the local political and social context (Eklöw & Mobjörk, 2024; Schipper, 2020).

  - *Recommendation 2: Promote Conflict-Sensitive Adaptation and Peace-Positive Climate Finance.* All climate adaptation projects in fragile contexts must be designed using a conflict-sensitive, "do no harm" lens. Conversely, climate finance should be strategically leveraged to generate "peace dividends" by explicitly supporting projects that build cross-community cooperation, strengthen inclusive resource governance, and foster shared resilience (Eklöw & Mobjörk, 2024).

- *Gap 3: Insufficient Investment in Fragile Contexts***.** Fragile and conflict-affected states are, by definition, the most vulnerable to climate-security risks. Yet, they are often the most difficult environments in which to invest and are frequently bypassed by traditional climate finance due to perceived risks and lack of institutional capacity (U.S. Framework for Climate Resilience and Security, 2024; Eklöw & Mobjörk, 2024). This creates a critical investment gap precisely where the need is greatest.
  - *Recommendation 3: Bridge the Institutional and Financial Divide***.** International actors must create new and more flexible financing mechanisms specifically designed to operate in high-risk, low-capacity environments. This requires breaking down the institutional walls between climate, development, humanitarian, and peacebuilding actors to pool resources, share risks, and co-design interventions that build resilience at the nexus of these challenges. Furthermore, policy must move beyond top-down solutions by actively integrating local and indigenous knowledge and empowering local communities to design and lead adaptation and peacebuilding efforts that are legitimate and sustainable in their own context (Eklöw & Mobjörk, 2024).

7. CONCLUSION

Climate change is fundamentally reshaping the landscape of global security. This article has sought to move beyond the simple label of "threat multiplier" to systematically deconstruct the complex and cascading ways in which a warming climate undermines human and state security. The evidence demonstrates that the pathway from a climate shock to violent conflict is not direct or inevitable, but is mediated through a chain of interconnected crises, with the quality of governance standing out as the most critical variable determining a society's fate.

The analysis presented in this article confirms that climate change acts as a threat multiplier through a sequence of cascading impacts. The process begins with first-order impacts on the physical environment, most notably the intensification of resource scarcity. As demonstrated by the case studies of water stress in the MENA region and food insecurity in Sub-Saharan Africa and South Asia, climate change is directly degrading the essential resource base—water, land, and food—upon which societies depend.

This resource pressure triggers second-order impacts in the form of human consequences, chief among them being climate-induced migration and displacement. As livelihoods in rural areas collapse, millions are compelled to move, as seen in the Sahel, Bangladesh, and Central America. This mass movement creates its own set of challenges, from immense strain on urban centers to a profound protection gap in international law for those displaced across borders.

Finally, in societies already burdened by fragility, these combined pressures can escalate into third-order crises of political instability and violent conflict. The case studies of Syria and Sudan serve as powerful, albeit tragic, illustrations of this entire causal chain. In both instances, severe, climate-exacerbated drought combined with decades of political mismanagement and pre-existing social grievances to create the conditions for catastrophic civil war. They underscore the central finding that climate stress becomes a catalyst for mass violence primarily when it intersects with weak, predatory, or biased governance.

The primary conclusion drawn from this analysis is that siloed policy approaches to this multifaceted challenge are destined to fail. A climate adaptation policy that ignores local conflict dynamics risks maladaptation, potentially creating more conflict than it solves. A security policy that ignores the underlying climate and environmental drivers of instability is merely treating symptoms, engaging in an endless and costly cycle of reactive crisis management. A development or humanitarian policy that does not account for future climate risks is unsustainable.

True, lasting security in the 21st century can only be achieved through a deeply integrated approach. Climate adaptation, sustainable development, and conflict prevention and peacebuilding must be seen not as separate policy domains, but as three essential and mutually reinforcing pillars of a single, coherent strategy for building resilient societies. This requires breaking down the institutional, financial, and conceptual walls that currently separate these fields of practice.

While our understanding of the climate-security nexus has advanced significantly, critical gaps remain. This article concludes by proposing several key avenues for future research that can help inform more effective policy and practice:

- *Evaluating Intervention Effectiveness*: There is a pressing need for more empirical, field-based research that critically evaluates the effectiveness of climate-security interventions. This should include a focus on identifying and understanding the potential for unintended negative consequences or maladaptation in climate adaptation and environmental peacebuilding projects (Eklöw & Mobjörk, 2024).
- *The Role of Local and Hybrid Peacebuilding*: Deeper investigation is needed into the role that local, traditional, and hybrid peacebuilding mechanisms play in successfully mediating climate-related resource conflicts. Understanding how to support and strengthen these indigenous capacities, rather than imposing external models, is crucial (Eklöw & Mobjörk, 2024).
- *Comparative Political Systems*: More systematic, comparative analysis is required to understand how different types of political systems—for instance, democratic versus authoritarian regimes—mediate climate-security risks differently. This could yield vital insights into the specific governance attributes that foster resilience.
- *Advancing Coupled Social-Climate Models*: Continued investment in the development of coupled social-climate models is essential. These models, which capture the two-way feedback loops between social dynamics like inequality and political polarization and physical climate outcomes, represent a vital frontier for understanding the deep integration of human and Earth systems (Menard et al., 2021; Koubi et al., 2022).

Addressing the security implications of climate change is one of the most formidable challenges of our time. It demands not only technical solutions and financial investment but also a fundamental shift in how we understand and practice security, moving from a paradigm of threat management to one of building shared, sustainable, and positive peace on a changing planet.

REFERENCES

Alianza MX. (2025). *Climate refugees in Northern and Central America*. University of California.

American Security Project. (2019). *Climate change, migration, and the Northern Triangle*.

Barnett, J. (2007). *Environmental security and peace*. Routledge.

Bouchaou, L., et al. (2024). Agricultural water use and demand assessment of the Souss basin, Morocco. *Frontiers in Water*, *6*.

Brown, O., & McLeman, R. (2009). A recurring anarchy? The emergence of climate change as a threat to international peace and security. *Conflict, Security & Development*, *9*(3), 289-316.

Busby, J. (2018). *Warming world: The new foreign policy challenges*. Center for a New American Security.

Carnegie Endowment for International Peace. (2024). *Climate change and conflict: A perfect storm in Sudan's countryside*.

Chatham House. (2024). *Tackling trade-related water risks: Case study Morocco*.

CNA Military Advisory Board. (2007). *National security and the threat of climate change*.

Copernicus SESA. (n.d.). *Climate Security*.

Dalby, S. (2024). The US national security community's threat multiplier frame: A dismal and limited worldmaking project. *ISA GSQ*, *4*(4).

de Châtel, F. (2014). The role of drought and climate change in the Syrian uprising: Untangling the triggers of the revolution. *Middle Eastern Studies*, *50*(4), 521-535.

de Soysa, I., & Rustad, S. A. (2010). *Climate change and conflict in Darfur*. CMI.

Detges, A. (2017). *Climate and conflict: Reviewing the statistical evidence*. adelphi.

Displacement Solutions. (2012). *Climate displacement in Bangladesh*.

Eklöw, K., & Mobjörk, M. (2024). Climate change and peacebuilding: sub-themes of an emerging research agenda. *International Affairs*, *100*(3), 1111-1129.

European Parliament. (2021). *The concept of 'climate refugee'*.

European Union. (2008). *Climate change and international security*. Paper from the High Representative and the European Commission to the European Council.

European Union. (2023). *Joint Communication on a new outlook on the climate and security nexus*.

Femia, F., & Werrell, C. (2012). *The Arab Spring and climate change*. Center for American Progress.

Food and Agriculture Organization of the United Nations (FAO). (2025). *Climate change and food security in sub-Saharan Africa*.

Gao, Y., et al. (2022). Modelling armed conflict risk under climate change with machine learning and time-series data. *Nature Communications*, *13*(1), 2416.

Gleick, P. H. (2014). Water, drought, climate change, and conflict in Syria. *Weather, Climate, and Society*, *6*(3), 331-340.

Global Governance Forum. (2022). *No status, no safety: Climate migrants in legal limbo*.

Goodman, S. (2023). *Threat multiplier: Climate, military leadership, and the fight for global security*. Island Press.

Hagel, C. (2014). *Hagel to address 'threat multiplier' of climate change*. U.S. Department of Defense.

Homer-Dixon, T. F. (1994). Environmental scarcities and violent conflict: Evidence from cases. *International Security*, *19*(1), 5-40.

IIED. (2025). *The vicious cycle pushing Bangladeshi climate migrants into modern slavery*.

IMF. (2022). *Climate change is intensifying food insecurity across sub-Saharan Africa*.

IOM. (2023). *Climate change and migration*.

Intergovernmental Panel on Climate Change (IPCC). (2022). *Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change*. Cambridge University Press.

Kahl, C. H. (2006). *States, scarcity, and civil strife in the developing world*. Princeton University Press.

Karmaoui, A., et al. (2019). Climate change impacts on water resources in the Souss-Massa basin, Morocco. *Procedia Manufacturing*, *32*, 533-540.

Kelley, C. P., et al. (2015). Climate change in the Fertile Crescent and implications of the recent Syrian drought. *Proceedings of the National Academy of Sciences*, *112*(11), 3241-3246.

Koubi, V. (2019). Climate change and conflict. *Annual Review of Political Science*, *22*, 343-360.

Koubi, V., et al. (2022). The effects of climate variability on conflict: A quantitative review. *Journal of Conflict Resolution*, *66*(1), 3-32.

Koubi, V., et al. (2024). Climate change and violent conflict: A critical review of the empirical literature. *WIREs Climate Change*, *15*(1), e863.

Menard, J., et al. (2021). When conflicts get heated, so does the planet: coupled social-climate dynamics under inequality. *Proceedings of the Royal Society B*, *288*(1959), 20211357.

Mixed Migration Centre. (2025). *Climate change and migration in the Central Sahel*.

Mobjörk, M., Krampe, F., & Tarif, K. (2020). Pathways of climate-related security risks: The case of Mali. *SIPRI*.

O'Loughlin, J., et al. (2014). The climate-conflict nexus: A comment on Hsiang and Meng. *Climatic Change*, *125*(1), 1-7.

Peace Agency. (2021). *Climate variability as a fuel to conflicts: The case of Syria*.

PLAN E. (2022). *Climate change isn't a threat multiplier. It's the main threat*. Defense One.

Plowman, J. A. (2011). *Climate change and conflict prevention: Lessons from Darfur*. National Defense University Press.

Read, P. (2021). Environmental security: An overview. *Scientia Militaria: South African Journal of Military Studies*, *49*(1), 42-60.

Red Cross. (n.d.). *Changing climate, changing realities: migration in the Sahel*.

Rigaud, K. K., et al. (2018). *Groundswell: Preparing for internal climate migration*. World Bank.

Schipper, E. L. F. (2020). Maladaptation: When adaptation to climate change goes wrong. *WIREs Climate Change*, *11*(1), e614.

Selby, J., et al. (2017). Climate change and the Syrian civil war revisited. *Political Geography*, *60*, 232-244.

South Asia Times. (2025). *Climate change & food security in South Asia*.

Sowers, J., Vengosh, A., & Weinthal, E. (2011). Climate change, water resources, and the politics of adaptation in the Middle East and North Africa. *Climatic Change*, *104*(3-4), 599-627.

Teka, O., et al. (2024). Climate change and food security in Sub-Saharan Africa: A review of adaptation strategies. *International Journal of Global Environmental Issues*, *23*(1), 37-57.

The Wave. (2025). *There's no legal definition of a climate refugee - does that matter?*.

The White House. (2022). *National Security Strategy*.

Theisen, O. M., Gleditsch, N. P., & Buhaug, H. (2013). Is climate change a driver of armed conflict? *Climatic Change*, *117*(3), 613-625.

UN Climate Security Mechanism (CSM). (2022). *Progress Report 2022*.

UN News. (2021). *Africa must tap into land restoration opportunities, says new UN-backed report*.

UNDP. (1994). *Human Development Report 1994*. Oxford University Press.

UNFCCC. (n.d.). *Climate Security Mechanism (CSM)*.

UNHCR. (2021). *Forced displacement related to the impacts of climate change and disasters*.

UNSSC. (2021). *Joint efforts for sustaining peace: Meet the UN Climate Security Mechanism*.

U.S. Framework for Climate Resilience and Security. (2024). *U.S. Framework for Climate Resilience and Security*.

van Baalen, S., & Mobjörk, M. (2018). Climate change and violent conflict in East Africa: Integrating qualitative and quantitative research to unfold the mechanisms. *Journal of Peace Research*, *55*(2), 153-167.

von Uexkull, N., & Buhaug, H. (2021). Security implications of climate change: A decade of scientific progress. *Journal of Peace Research*, *58*(1), 3-17.

WFP. (2016). *Climate change and food security*.

WFP USA. (2021). *Climate change, food security, and humanitarian emergencies*.

World Bank. (2021). *Groundswell Part 2: Acting on Internal Climate Migration*. World Bank.

World Bank. (2023). *Climate and Development: An Agenda for Action*. World Bank.

World Bank. (2024). *Population mobility in the Sahel: Implications for adaptive social protection*.

World Bank. (2025). *Building a water-secure future in the Middle East and North Africa*.

Zittis, G., et al. (2021). Projected changes in extreme heatwaves over the Middle East and North Africa (MENA) in a 2°C and 4°C warmer world. *Climatic Change*, *169*(1-2), 1-20.

THE GEOPOLITICS OF CYBERSECURITY: A COMPARATIVE ANALYSIS OF NATIONAL STRATEGIES FOR DIGITAL SOVEREIGNTY

Oksana Prokopyshyn
Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies Lviv
Lviv, Ukraine
https://orcid.org/0000-0002-7027-3499

Nataliia Trushkina
Research Center for Industrial Problems of Development of the NAS of Ukraine
Kharkiv, Ukraine
https://orcid.org/0000-0002-6741-7738

Abstract. *This paper investigates the divergent national strategies for achieving "digital sovereignty" among four major geopolitical actors: the United States, the European Union, China, and Russia. It argues that digital sovereignty has evolved from a defensive concept focused on network security into a comprehensive geopolitical strategy for projecting power, values, and economic influence (Süsslin, 2025; Metakides, 2025). Through a comparative analysis of key policy and legal frameworks—including the US National Cybersecurity Strategy (2023), the EU's GDPR/DSA/DMA package, China's Cybersecurity Law (CSL), and Russia's "Sovereign Internet" laws—the paper identifies three distinct models of digital sovereignty: the US market-driven, rebalanced-responsibility model; the EU's regulation-as-power, normative model; and the Sino-Russian state-centric, control-oriented model (Metakides, 2025; Freedom House, n.d.). The analysis reveals that these approaches are creating a fragmented "splinternet," characterized by competing regulatory blocs, contested data governance regimes, and a securitized global technology supply chain (Carnegie Endowment for International Peace, 2025). The paper concludes by proposing a new framework that understands digital sovereignty not merely as a quest for autonomy but as a primary vector for exercising state power in a multipolar digital world order, with significant implications for global stability, international law, and the future of the internet..*

Keywords: Digital Sovereignty, Geopolitics, Cybersecurity, Splinternet, Data Governance, US National Cybersecurity Strategy, EU GDPR, China Cybersecurity Law, Russia Sovereign Internet.

1. INTRODUCTION: THE RISE OF DIGITAL SOVEREIGNTY IN A FRACTURING CYBERSPACE

The early architecture of the internet was animated by a utopian vision of a borderless, global commons—a space for open communication, innovation, and connection that would transcend the physical constraints of the nation-state (The White House, 2023). This vision, however, has been progressively fractured. The contemporary digital ecosystem is a contested domain, increasingly defined by geopolitical tensions, the weaponization of synthetic media, and the normalization of cyber-enabled conflict (Center for Long-Term Cybersecurity, 2025; Palo Alto Networks, 2025). The result is not a single, global internet but an accelerating fragmentation into multiple "splinternets": a collection of isolated or semi-isolated networks controlled by governments, each with its own rules, standards, and values (Carnegie Endowment for International Peace, 2025). This trend signals a profound global shift in which, as some analysts have noted, "digital solidarity is out. Tech sovereignty is in" (Carnegie Endowment for International Peace, 2025).

This fragmentation is a direct consequence of states reasserting control over the digital sphere through the pursuit of "digital sovereignty." As a concept, digital sovereignty is both polysemic and politically charged (e.g., Couture & Toupin, 2019). At its core, it refers to the ability of a state or collective community to exercise control and autonomy over its digital infrastructure, data flows, and the foundational technologies that underpin its economy and society (e.g., Couture & Toupin, 2019; Süsslin, 2025). This pursuit is not necessarily for complete technological self-sufficiency but for strategic autonomy in critical areas to protect national interests, security, and economic prosperity (Süsslin, 2025). The concept is now mobilized by a diverse range of actors, from liberal democracies seeking to protect citizens' rights to authoritarian states aiming to consolidate control, making it a central battleground in 21st-century geopolitics (e.g., Couture & Toupin, 2019; Metakides, 2025).

The impetus for this global turn towards digital sovereignty is deeply rooted in a pervasive sense of geopolitical insecurity. The digital domain has become a primary theater for great power competition, and the shockwaves of terrestrial conflicts are felt acutely in cyberspace (Munich Security Conference, 2022; Palo Alto Networks, 2025). The Russian invasion of Ukraine, for instance, was accompanied by cyberattacks and sparked widespread fears of digital escalation against NATO states, heightening distrust between geopolitical blocs (Munich Security Conference, 2022). In this "tumultuous moment in history," where the rules-based international order is under assault, digital dependencies have transformed from assets into profound vulnerabilities (Munich Security Conference, 2022; Institute for Defense Analyses, 2023). The push to erect "digital walls" (Carnegie Endowment for International Peace, 2025) and build digital fortresses is a direct response to this volatility, representing a state's attempt to regain a measure of security and predictability in an environment where its digital lifelines are exposed to foreign manipulation and disruption.

This paper advances the thesis that national strategies for digital sovereignty are not merely reactive, technical cybersecurity policies. They are proactive, comprehensive geopolitical projects that reflect and project distinct ideological values, economic models, and visions of world order. These strategies represent a fundamental reassertion of the state in the digital age, challenging the once-dominant multi-stakeholder model of internet governance (ResearchGate, 2021). By conducting a comparative analysis of the strategic approaches of the United States (US), the European Union (EU), the People's Republic of of China (PRC), and the Russian Federation, this paper will demonstrate how these competing visions are actively shaping the future of cyberspace (Metakides, 2025; Freedom House, n.d.). It will argue that these divergent paths are creating a multipolar digital world, with profound implications for international law, global trade, and the very architecture of the internet.

2. THEORETICAL FRAMEWORK: SOVEREIGNTY, POWER, AND REGULATION IN THE DIGITAL AGE

To analyze the complex interplay of forces shaping national digital sovereignty strategies, this paper employs a multidisciplinary theoretical framework drawing from International Relations (IR), law, political economy, and Science and Technology Studies (STS) (Martino & Gamal, 2022). This framework provides the analytical lens to deconstruct and compare the divergent approaches of the US, EU, China, and Russia.

The analysis is grounded in the classical concept of Westphalian sovereignty, which posits the state's exclusive and supreme authority within its defined territorial boundaries (Werthner, 2025). The central debate in the geopolitics of cybersecurity revolves around whether and how this principle can be extended into the intangible, non-territorial realm of cyberspace (Werthner, 2025; Süsslin, 2025). This question frames the fundamental ideological clash between the state-centric model of governance, championed by China and Russia, and the multi-stakeholder model, historically promoted by the United States and civil society organizations (Süsslin, 2025; ResearchGate, 2021). The former sees the internet as a space to be governed by sovereign states to protect national security and public order, while the latter envisions a decentralized ecosystem managed by a diverse group of actors, including industry, academia, and non-governmental organizations (ResearchGate, 2021).

To understand the EU's unique strategy, this paper utilizes the concepts of "regulatory mercantilism" and the "Brussels Effect" (Süsslin, 2025; PromethEUs, 2023). Regulatory mercantilism describes how states use regulations, standards, and certifications not only for domestic policy goals but also as tools of economic and geopolitical competition (Süsslin, 2025). The "Brussels Effect" is a specific manifestation of this, whereby the EU leverages its large, attractive single market to externalize its legal and regulatory norms globally (PromethEUs, 2023). Landmark regulations like the General Data Protection Regulation (GDPR) compel multinational corporations to adopt EU standards worldwide to access the European market, effectively allowing the EU to project power and shape global business practices without resorting to traditional military or economic coercion (PromethEUs, 2023). This makes regulation itself a primary instrument of the EU's pursuit of digital sovereignty.

For China's approach, the framework of "rule by law" provides a critical distinction from the Western concept of the "rule of law" (U.S.-China Economic and Security Review Commission, 2023). In a "rule by law" system, law is not an independent constraint on state power but rather a primary instrument for the ruling party—in this case, the Chinese Communist Party (CCP)—to implement its policies and achieve its strategic objectives (U.S.-China Economic and Security Review Commission, 2023). This includes maintaining social control, directing economic development, and projecting influence internationally. This legal philosophy is inextricably linked to the rise of techno-authoritarianism, where the state deploys advanced surveillance and control technologies, justified and enabled by a comprehensive legal architecture. China actively exports this governance model through initiatives like the Digital Silk Road, offering technology and training to other nations, thereby shaping global norms to reflect its own state-centric, control-oriented vision (ResearchGate, 2021; U.S.-China Economic and Security Review Commission, 2023).

Finally, adopting a perspective from STS, this paper views sovereignty not merely as an abstract legal claim but as a tangible reality that is actively constructed, or "infrastructured" (Musiani et al., 2019). Digital sovereignty is realized through the co-construction of policy, legal frameworks, technical standards, and physical infrastructures. To understand a nation's strategy, one must analyze not only its laws and doctrines but also the material components that enforce them: the development of national data centers, control over encryption standards and internet routing protocols, and the management of the physical conduits of data flow like subsea cables and data ports (Musiani et al., 2019; MERICS, 2023).

A nation's approach to digital sovereignty is thus best understood as an inseparable trinity of its technological capacity, its legal-regulatory philosophy, and its core political ideology. These three elements are mutually constitutive and cannot be analyzed in isolation. The EU's relative weakness in the platform economy, for example, necessitates its heavy reliance on regulatory power to govern the dominant US and Chinese tech giants—a form of asymmetric statecraft (PromethEUs, 2023; McKinsey & Company, 2022). Conversely, China's ability to implement its "Great Firewall" and comprehensive surveillance systems depends on possessing both the legal mandate from its Cybersecurity Law and the indigenous technological capacity of companies like Huawei and Alibaba to build and operate these systems (U.S.-China Economic and Security Review Commission, 2023; MERICS, 2020). The law justifies the technology, the technology enforces the law, and both serve the CCP's ideological goal of comprehensive control. This integrated trinity forms the fundamental unit of analysis for comparing the national strategies that follow.

3. COMPARATIVE ANALYSIS OF NATIONAL STRATEGIES FOR DIGITAL SOVEREIGNTY

The divergent paths taken by the United States, the European Union, China, and Russia in their pursuit of digital sovereignty have given rise to distinct, and often conflicting, models of digital governance (Couture & Toupin, 2019; Freedom House, n.d.). These models are not merely technical frameworks but are deeply embedded in each actor's unique political culture, economic structure, and geopolitical ambitions. An examination of their core doctrines and key legal instruments reveals a fragmenting global digital order.

Table 1: A Comparative Framework of National Digital Sovereignty Strategies

Dimension	United States	European Union	People's Republic of of China	Russian Federation
Core Doctrine	Market-Driven Security & Rebalanced Responsibility (The White House, 2023)	Normative Power & Strategic Autonomy (Metakides, 2025; PromethEUs, 2023)	Cyber Sovereignty & Comprehensive State Control (Cheng & Liu, 2022; Freedom House, n.d.)	Defensive Sovereignty & Digital Fortress (ResearchGate, 2021)
Key Legal/Policy Instruments	National Cybersecurity Strategy (2023) (The White House, 2023), CLOUD Act (The Belfer Center for Science and International Affairs, 2021), Sector-specific regulations (Süsslin, 2025)	GDPR, Digital Services Act (DSA), Digital Markets Act (DMA), AI Act, NIS2 Directive (PromethEUs, 2023; European Parliament, 2025)	Cybersecurity Law (CSL), Data Security Law (DSL), PIPL, "Great Firewall" (MERICS, 2023; Freedom House, n.d.)	"Sovereign Internet Law," (ResearchGate, 2021) Data Localization Laws (FZ-242) (Gorodissky & Partners, 2023)
Primary Goal	National & Economic Security (Galinec et al., n.d.)	Protection of Fundamental Rights & Single Market Integrity (PromethEUs, 2023; European Parliament, 2025)	Regime Stability & Social Control (U.S.-China Economic and Security Review Commission, 2023; Freedom House, n.d.)	Regime Stability & Insulation from External Pressure (ResearchGate, 2021; Freedom House, n.d.)
Approach to Data Governance	Sector-specific, market-led, with a shift towards federal privacy law (The White House, 2023; Süsslin, 2025)	Comprehensive, rights-based, extraterritorial ("Brussels Effect") (Süsslin, 2025; PromethEUs, 2023)	State-centric, data as a national asset, strict localization (MERICS, 2023)	Strict data localization, state control over data flows (Gorodissky & Partners, 2023)
Stance on Global Internet Governance	Historically multi-stakeholder, now with a stronger emphasis on national interest and security (U.S.-China Economic and Security Review Commission, 2023; The White House, 2023)	Multi-stakeholder, but shaped by EU values and regulations (PromethEUs, 2023)	State-centric, promoting "cyber sovereignty" at the UN/ITU (ResearchGate, 2021; U.S.-China Economic and Security Review Commission, 2023)	State-centric, actively disrupting the multi-stakeholder model (ResearchGate, 2021)

3.1. THE UNITED STATES: A MARKET-DRIVEN ECOSYSTEM WITH REBALANCED RESPONSIBILITY

The US approach to cybersecurity and digital sovereignty has historically been characterized by a reliance on market forces, public-private partnerships, and a sector-specific regulatory model (The White House, 2023; SIPRI, 2024). The 2023 National Cybersecurity Strategy (NCS) represents a significant evolution of this approach, introducing a new philosophy centered on two fundamental shifts: rebalancing responsibility and realigning incentives (Institute for Defense Analyses, 2023; The White House, 2023). This strategy explicitly recognizes that the burden of cybersecurity has fallen disproportionately on individual users and small organizations (The White House, 2023). It seeks to shift this responsibility to the actors most capable of bearing it: large-scale technology providers and the owners and operators of critical infrastructure (The White House, 2023).

The strategy is structured around five pillars that operationalize this vision (Institute for Defense Analyses, 2023; The White House, 2023; Galinec et al., n.d.; Federal Communications Commission, 2023):

1. Defend Critical Infrastructure: This involves expanding the use of minimum cybersecurity requirements for critical sectors and strengthening public-private collaboration (The White House, 2023).
2. Disrupt and Dismantle Threat Actors: This calls for a more proactive, integrated use of all instruments of national power—diplomatic, military, intelligence, and law enforcement—to make malicious cyber activities costly and unsustainable for adversaries (The White House, 2023).
3. Shape Market Forces to Drive Security and Resilience: This is arguably the most innovative pillar. It proposes using federal procurement power and potential legislation to shift liability onto providers of insecure software products and services, thereby creating powerful market incentives for building security in by design (The White House, 2023).
4. Invest in a Resilient Future: This pillar focuses on long-term investments in a secure technical foundation for the internet, R&D for next-generation technologies like post-quantum cryptography, and strengthening the national cyber workforce (The White House, 2023; Galinec et al., n.d.).
5. Forge International Partnerships to Pursue Shared Goals: This reaffirms the US commitment to working with allies to build coalitions, strengthen partner capacity, and reinforce global norms of responsible state behavior (The White House, 2023).

The US strategy is lauded in expert assessments for its forward-thinking vision on aligning private-sector incentives with security goals and for its robust framework for public-private partnerships (The Belfer Center for Science and International Affairs, 2025). However, it is also criticized for significant gaps, particularly in its lack of specific measures to protect individuals, their personal data, and vulnerable small- and medium-sized enterprises (SMEs) (The Belfer Center for Science and International Affairs, 2025). Geopolitically, the NCS is explicit, naming China as the "broadest, most active, and most persistent threat" and framing the global digital competition as a contest of values (The White House, 2023). It champions a vision of an "open, free, global, interoperable, reliable, and secure" internet (The White House, 2023; Institute for Defense Analyses, 2023). Yet, this official stance exists in tension with recent political trends suggesting a potential pivot towards a more transactional, "America First" approach to technology policy, which could prioritize American primacy over the principles of digital solidarity and international cooperation (Carnegie Endowment for International Peace, 2025).

3.2. THE EUROPEAN UNION: SOVEREIGNTY THROUGH NORMATIVE POWER AND REGULATION

The European Union has carved out a distinct "third way" in the global digital order, one that is neither the market-led model of the US nor the state-controlled model of China (Couture & Toupin, 2019; Metakides, 2025). The EU's strategy is to achieve "strategic autonomy" and "digital sovereignty" through the exercise of its formidable regulatory power (PromethEUs, 2023; Metakides, 2025). This approach is born from a clear-eyed assessment of its geopolitical position: while the EU is an economic heavyweight, it lacks homegrown technology giants on the scale of those in the US and China (McKinsey & Company, 2022). Consequently, it leverages its most powerful asset—its unified, high-value single market—to set the rules of the game for all actors who wish to operate within it (Süsslin, 2025; PromethEUs, 2023).

The EU's regulatory arsenal is comprehensive and continues to expand:

- The General Data Protection Regulation (GDPR) is the backbone of this strategy. Enacted in 2018, it established a global "gold standard" for data protection, centering on the fundamental rights of individuals (PromethEUs, 2023). Its extraterritorial scope forces companies worldwide to comply with EU norms, demonstrating the "Brussels Effect" in action (Süsslin, 2025; PromethEUs, 2023).

- The Digital Services Act (DSA) and Digital Markets Act (DMA), which became fully applicable in 2024, extend this regulatory reach to the largest online platforms, designated as "gatekeepers" (e.g., European Parliament, 2025; Hausfeld, 2022; European Commission, n.d.). The DSA imposes new responsibilities for content moderation to create a safer online environment, while the DMA introduces pro-competitive rules to ensure fairness and contestability in digital markets, directly targeting the business models of non-EU tech giants (PromethEUs, 2023; European Parliament, 2025; Hausfeld, 2022).
- The AI Act and Cyber Resilience Act represent the next wave of this strategy, embedding regulatory requirements into emerging technologies from the outset. The AI Act establishes a risk-based framework for artificial intelligence, while the Cyber Resilience Act mandates security standards for all products with digital elements (PromethEUs, 2023; European Parliament, 2025).

Underpinning these laws is a coherent data governance strategy aimed at creating "sovereign data ecosystems" (PromethEUs, 2023). The Data Governance Act (DGA) and the Data Act (DA) establish frameworks for increasing trust and facilitating data sharing within and between sectors, envisioning common European data spaces for health, energy, and public administration (PromethEUs, 2023). This is a deliberate effort to foster a data-driven European economy that operates according to EU values of privacy, security, and fairness (PromethEUs, 2023; European Data Protection Supervisor, 2025).

3.3. CHINA: CYBER SOVEREIGNTY AS AN INSTRUMENT OF COMPREHENSIVE STATE CONTROL

China's approach to the digital domain is the most explicit and comprehensive articulation of state-centric control. Its guiding doctrine is "cyber sovereignty" (网络主权, wǎngluò zhǔquán), which posits that cyberspace is a domain of national sovereignty, equivalent to land, sea, and air, and therefore subject to the absolute authority of the state (U.S.-China Economic and Security Review Commission, 2023; ResearchGate, n.d.; Cheng & Liu, 2022). This doctrine is not primarily about protecting individual rights but about safeguarding national security, ensuring social stability, and cementing the political power of the CCP (U.S.-China Economic and Security Review Commission, 2023).

This doctrine is operationalized through a powerful legal triad:

- The Cybersecurity Law (CSL) of 2017 is the foundational legislation. It establishes broad, and often vaguely defined, security obligations for "network operators" and "critical information infrastructure operators" (CIIOs), giving the state extensive powers of supervision and inspection (ResearchGate, n.d.; Cheng & Liu, 2022; Süsslin, 2025; Freedom House, n.d.; Alkan, 2012).
- The Data Security Law (DSL) of 2021 builds on the CSL by creating a hierarchical system for data classification. Data is categorized based on its importance to national security and public interest, with the strictest controls applied to "national core data" and "important data" (MERICS, 2023).
- The Personal Information Protection Law (PIPL) of 2021 is China's analogue to the GDPR. While it grants individuals rights regarding their personal data, these rights are subordinate to the state's interests (Süsslin, 2025). The law contains broad national security exemptions and mandates state access to data, reflecting the "rule by law" philosophy where individual rights are granted by the state and can be curtailed for state purposes (Süsslin, 2025; U.S.-China Economic and Security Review Commission, 2023).

The enforcement of this legal regime relies on two powerful mechanisms: the "Great Firewall" and strict data localization requirements. The Great Firewall is far more than a simple censorship tool; it is a sophisticated system for controlling the entirety of China's digital environment, managing cross-border data flows, filtering content, and blocking access to foreign services (Carnegie Endowment for International Peace, 2025; MERICS, 2023; Mirrlees, 2022). This is complemented by stringent data localization rules under the CSL and DSL, which mandate that all personal information and "important data" generated within China must be stored on domestic servers (MERICS, 2023). This ensures the state has unfettered access to and jurisdiction over the data, effectively creating a "state-controlled data island"

(MERICS, 2023). China actively exports this model of cyber governance globally through its Digital Silk Road initiative and by providing training and technology to officials from other countries, promoting an alternative, authoritarian vision for the future of the internet (ResearchGate, 2021; U.S.-China Economic and Security Review Commission, 2023).

3.4. RUSSIA: THE SOVEREIGN INTERNET AS A DEFENSIVE DIGITAL FORTRESS

Russia's strategy for digital sovereignty is primarily defensive and, in many respects, isolationist. It is driven by a deep-seated fear of Western political and cultural influence, the potential for foreign-instigated "color revolutions," and a paramount desire to ensure regime stability (ResearchGate, 2021; Freedom House, n.d.). The overarching goal is to insulate the Russian domestic internet segment, known as the "Runet," from external pressures and to guarantee its continued operation even in the event of a disconnection from the global internet (Litvinenko, 2021; ResearchGate, 2021).

The centerpiece of this strategy is the "Sovereign Internet Law" (Federal Law No. 90-FZ), which came into force in 2019 (ResearchGate, 2021). This legislation mandates the creation of a national Domain Name System (DNS) to reduce reliance on international servers. More critically, it requires all domestic internet traffic to be routed through state-controlled exchange points managed by the telecommunications regulator, Roskomnadzor (ResearchGate, 2021). This provides the state with the technical infrastructure necessary to monitor, filter, block, and potentially isolate the Runet from the outside world, creating a "digital fortress."

Like China, Russia enforces strict data localization rules. Federal Law No. 242-FZ, enacted in 2015, requires that any company, foreign or domestic, that collects the personal data of Russian citizens must store and process that data on servers physically located within the Russian Federation (Gorodissky & Partners, 2023; Hivenet, n.d.; Captain Compliance, 2025). This law is a clear assertion of jurisdictional sovereignty, ensuring that the data of its citizens remains within the legal reach of Russian authorities and security services (Hivenet, n.d.). Non-compliance has led to significant fines and the blocking of services like LinkedIn (Gorodissky & Partners, 2023).

While Russia and China are often grouped together as proponents of state-centric "digital sovereignty," their approaches have notable differences (ResearchGate, 2021). Russia's strategy is less technologically and economically integrated than China's. It is more narrowly focused on control and insulation, reflecting a less developed domestic technology sector and a more confrontational diplomatic posture (ResearchGate, 2021; Freedom House, n.d.; U.S. Department of State, 2023). In international forums, Russia often plays the role of the primary disruptor of the multi-stakeholder model, while China pursues a more patient, long-term strategy of building an alternative ecosystem and sphere of influence (ResearchGate, 2021).

4. DISCUSSION: THEMATIC CONTESTS IN THE GEOPOLITICS OF CYBERSPACE

The implementation of these divergent national strategies is not occurring in a vacuum. They collide in key arenas of the global digital ecosystem, creating new forms of geopolitical contestation. The battle for digital sovereignty is being waged over data flows, through global supply chains, and in the race for technological supremacy.

4.1. THE BATTLE FOR DATA: FLOWS VS. FORTRESSES

At the heart of the geopolitical struggle is a fundamental conflict over the governance of cross-border data flows. This contest pits models that favor the free, albeit regulated, flow of data against those that prioritize data localization and state control. The EU's GDPR exemplifies a conditional flow model, permitting data transfers only to jurisdictions that provide an "adequate" level of protection, effectively exporting its standards (PromethEUs, 2023). The US has historically advocated for a more liberal, market-driven approach to data flows, though this is increasingly being tempered by national security concerns (Süsslin, 2025).

In stark contrast, China and Russia have erected digital fortresses built on strict data localization mandates (MERICS, 2023; Gorodissky & Partners, 2023). These policies require that citizen data and other categories of "important data" be stored domestically, which serves the dual purpose of asserting sovereign jurisdiction and ensuring state access for security and surveillance purposes (Hivenet, n.d.; The Belfer Center for Science and International Affairs, 2021). This approach is often justified on grounds of protecting national security and citizen privacy from foreign surveillance (Hivenet, n.d.). However, critics argue that such measures are often a tool for digital authoritarianism, enabling greater government control over information and stifling dissent (Hivenet, n.d.). Economically, data localization can impose significant costs, increase regulatory complexity, and handicap innovation by creating barriers to the global data exchange that fuels modern business (The Belfer Center for Science and International Affairs, 2021). This clash of data governance philosophies is a primary driver of the internet's fragmentation, creating a "balkanized" global landscape where data cannot move freely across competing regulatory blocs (PromethEUs, 2023).

4.2. THE SECURITIZATION OF GLOBAL SUPPLY CHAINS

The competition for digital sovereignty has expanded beyond data and software to encompass the physical hardware and supply chains that form the backbone of the digital world. Advanced technologies, particularly semiconductors, are no longer viewed merely as commercial products but as "sovereign assets" fundamental to national security (Center for Long-Term Cybersecurity, 2025). This has led to the deep securitization of global technology supply chains.

The US has been at the forefront of this trend, with policies like the CHIPS and Science Act and escalating sanctions against China's technology industry. These are not just economic measures; they are explicit national security strategies designed to slow China's technological advancement and secure US leadership in critical technologies (Center for Long-Term Cybersecurity, 2025; Mirrlees, 2022). This approach is not unique to the US. The EU, China, and Russia are all implementing measures to vet, limit, or prohibit foreign hardware and software in their critical infrastructure and government systems (SIPRI, 2024). China's "document 79" initiative, for example, reportedly aims to replace foreign technology in state-owned enterprises, while Russia has banned foreign software from its critical infrastructure facilities (SIPRI, 2024). The EU's NIS2 Directive and other regulations include provisions for assessing supply chain risks, including the potential for "undue influence by a third country on suppliers" (SIPRI, 2024). This transforms international trade in technology into a key battleground of geopolitical competition, where trust is low and every component is potentially suspect.

4.3. THE RACE FOR TECHNOLOGICAL SUPREMACY: AI AND QUANTUM

Emerging and foundational technologies, especially artificial intelligence (AI) and quantum computing, represent the new high ground in geopolitical competition. Leadership in these fields is seen as essential not only for future economic prosperity but also for national security and military advantage (Center for Long-Term Cybersecurity, 2025; Winslow, 2025; World Health Organization, 2020). The rapid advancement of these technologies has triggered a global race for supremacy, with enormous stakes.

This race is unfolding across multiple dimensions. Nations are pouring vast resources into R&D, as seen in the US strategy's call to reinvigorate federal research and China's massive state-backed investments (The White House, 2023; Creemers, 2020; National Development and Reform Commission, 2021). They are also developing divergent approaches to governance. The EU is pioneering a risk-based, human-centric regulatory model with its AI Act, seeking to ensure that AI development aligns with democratic values (PromethEUs, 2023; European Parliament, 2025). In contrast, China's approach is state-driven, focused on rapid deployment for economic gain and social management, integrating AI into its surveillance and control apparatus (U.S.-China Economic and Security Review Commission, 2023; MERICS, 2020). The geopolitical implications are profound, as these technologies can be used to power sophisticated cyberattacks, conduct influence operations with deepfakes, or achieve decisive military superiority (Center for Long-Term Cybersecurity, 2025; Winslow, 2025; Belli, 2025). The looming threat of a cryptographically relevant quantum computer—one capable of breaking current encryption standards—adds another layer of urgency, forcing nations to prepare for a "post-quantum future" where today's secure data could become transparent (The White House, 2023; Center for Long-Term Cybersecurity, 2025; KPMG, 2025).

This intense pursuit of digital sovereignty, while intended to bolster national security, is paradoxically cultivating new and systemic global vulnerabilities. The fragmentation of the internet into distinct "splinternets" and "data islands" dramatically increases the complexity of the global digital ecosystem (Carnegie Endowment for International Peace, 2025; MERICS, 2023; Winslow, 2025). This complexity is not merely an inconvenience; it is a source of strategic risk. As multinational corporations are forced to splinter their data systems to comply with a patchwork of conflicting regulations, the operational overhead and potential for error increase (MERICS, 2023). This environment fosters a "cyber inequity," where smaller organizations, often critical links in global supply chains, lack the resources to navigate the complex regulatory landscape and maintain robust security, creating weak points that adversaries can exploit (Winslow, 2025). Furthermore, in a crisis, the lack of interoperability and shared norms between these fragmented blocs would severely hamper a coordinated international response to a major cyber incident. The digital walls built for defense could easily become the walls of a prison, isolating nations and making it harder to fight a common, sophisticated threat. The very architecture of fragmentation creates seams and gaps, and in the "fog of war" of a major cyber conflict, these seams are precisely where catastrophic failures are most likely to occur (Palo Alto Networks, 2025).

5. CONCLUSION: PROJECTING POWER IN A DIVIDED DIGITAL FUTURE

The evidence and analysis presented in this paper demonstrate that the concept of "digital sovereignty" has undergone a critical evolution. It has transformed from a primarily defensive posture, concerned with protecting national networks from external threats, into a proactive and increasingly offensive instrument for projecting national power in the 21st century. The strategies of the world's major digital actors are no longer just about building firewalls; they are about exporting influence, values, and economic models. The European Union projects its power through normative regulation, using the "Brussels Effect" to shape global markets in its image (PromethEUs, 2023). China projects its power by exporting its techno-authoritarian governance model via the Digital Silk Road, creating a sphere of influence aligned with its state-centric vision (ResearchGate, 2021; U.S.-China Economic and Security Review Commission, 2023). The United States continues to project power through the global dominance of its technology industry and its ability to shape market standards, now coupled with a more explicit strategy of leveraging market forces and liability to enforce security (The White House, 2023; Mirrlees, 2022).

This reality necessitates moving beyond the simplistic "open vs. closed" binary that has long dominated discussions of internet governance. The Cold War-era dichotomy of a free and "open" internet (led by the US and the West) versus a censored and "closed" internet (led by China and Russia) is no longer sufficient to describe the global landscape (Center for Long-Term Cybersecurity, 2025). The emergence of the EU as a distinct regulatory superpower has created a multipolar digital order with at least three competing poles (Metakides, 2025). The EU's model is neither fully open in the libertarian, market-led sense of the US, nor is it fully closed in the authoritarian, state-controlled sense of China. It represents a third, values-driven, regulatory-heavy approach that is actively shaping the behavior of the other two (Metakides, 2025; PromethEUs, 2023).

In this new multipolar digital world, the strategic alignment of "digital middle powers"—nations like India, Brazil, Nigeria, and Indonesia—becomes a decisive factor (Pannier, 2023). These countries are not just passive recipients of technology and norms; they are increasingly influential actors in their own right. Their strategic choices—which model to emulate, which standards to adopt, or whether to forge their own hybrid approaches—will determine the future balance of power in global digital governance. The competition for their allegiance is the new geopolitical prize, and their decisions will shape the contours of the splinternet for decades to come.

The scientific novelty of this paper lies in its reframing of digital sovereignty not as a niche cybersecurity issue, but as a primary instrument of 21st-century statecraft, integrating legal, technological, economic, and ideological dimensions of power (Werthner, 2025). It provides a framework for understanding how states are competing to define the future of a digital world that is no longer global and unified, but fragmented and contested. This analysis opens several critical avenues for future research. First, there is a pressing need for empirical studies on how digital middle powers are navigating this geopolitical competition and formulating their own sovereign strategies (Pannier, 2023). Second, the fragmentation of the digital sphere requires the development of new international legal principles and diplomatic mechanisms for managing conflict and ensuring stability in a world without a single, universally accepted set of rules. Finally, continued analysis of the long-term impact of the technological race, especially in AI and quantum computing, is essential for understanding its potential to either stabilize or destabilize the international system (Center for Long-Term Cybersecurity, 2025). The choices made today will determine whether the divided digital future is one of managed competition or perpetual conflict.

REFERENCES

Alkan, M. (2012). Cybersecurity governance models: A brief overview. *Information & Security: An International Journal, 38*(2), 58–66.

Arsène, S. (2019). The turn to sovereignty in internet governance. In F. Musiani, S. Arsène, C. O. de la Sablière, & C. T. (Eds.), *The turn to sovereignty in internet governance*.

BDO. (2024, September). *Top cybersecurity threats and predictions for 2025*.

Belli, L. (2025). *Cybersecurity and AI*.

Bendiek, A., & Scholl, P. (2024). The EU's strategic turn in cybersecurity: a case of regulatory mercantilism?. *International Affairs, 100*(6), 2379-2397.

Captain Compliance. (2025, January 6). *Russia Data Localization Law: 2025 Essential Guide*.

Carnegie Endowment for International Peace. (2025, May). *Digital democracy in a divided global landscape*.

Carroll, J. M. (2024). Secure Your Supply Chains: A Recipe for Building the Best Products. *Proceedings of the 23rd European Conference on Cyber Warfare and Security, ECCWS 2024*.

Center for Long-Term Cybersecurity (CLTC), UC Berkeley. (2025). *Reflections on cybersecurity futures 2025: Looking back from the present*.

China Aerospace Studies Institute. (2021, October). *U.S.-China Competition in AI*.

Cleary Gottlieb. (2022, October 27). *Digital Services Act Published in the EU Official Journal*. Cleary Antitrust Watch.

Couture, S., & Toupin, S. (2019). What does the notion of “digital sovereignty” stand for? A comparison of the terms used in the public debates of Canada, China, France, and Russia. *New Media & Society, 21*(10), 2319-2337.

Creemers, R. (2020). *China's approach to cyber sovereignty*. Konrad Adenauer Stiftung.

Davis Center for Russian and Eurasian Studies, Harvard University. (2021). *Digital Silk Road in Central Asia: Present and Future*.

European Commission. (n.d.). *The Digital Services Act*. Retrieved July 3, 2025, from https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

European Data Protection Supervisor (EDPS). (2025, March). *EDPS Mandate Review 2020–2024*.

European Liberal Forum. (2023). *The Digital Services Act (DSA): Between European autonomy and transatlantic cooperation*.

European Parliament. (2025, April). *Digital agenda for Europe*.

European Parliament. (2025). *The Recovery and Resilience Facility (RRF) and cybersecurity*.

European Union. (2022a). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). *Official Journal of the European Union, L 265*, 1-66.

European Union. (2022b). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union, L 277/1*.

Federal Communications Commission. (2023, July). *National Cybersecurity Strategy*.

Freedom House. (n.d.). *Freedom on the Net Reports*.

Future of Privacy Forum. (2022, June). *Chinese Data Protection in Transition*.

Google Cloud. (2025). *Cybersecurity Forecast 2025*.

Gorodissky & Partners. (2023). *Data protection in the Russian Federation: overview*.

Government of Malta. (2023). *Maltese National Cybersecurity Strategy 2023-2026*.

Hausfeld. (2022, November 1). *The EU Digital Markets Act*.

Hernández, S., & Raina, A. (2020). Legal problems with data localization requirements: The case of the Russian Federation. *Global Trade and Customs Journal, 15*(9), 445–459.

Hivenet. (n.d.). *Does national pride win over innovation? The contradictions in data localization*.

Hunton Andrews Kurth LLP. (2023). *2023 Data Protection and Privacy: Introduction*.

Institute for Defense Analyses. (2023). *Summary of National Cybersecurity Strategy with Similarity Analysis to Executive Order 14028*.

International Trade Administration. (n.d.). *Challenges of the Chinese eCommerce Market*. U.S. Department of Commerce.

James Cook University. (2020). *Research Data & Information Management Framework 2020-2025*.

KPMG. (2025, June). *Cyber considerations 2025*.

Lee, T.-L. (2025, February). Digital health governance: Technological solutionism, human rights, and data sovereignty. *European Journal of Legal Studies, Special Issue*, 101-159.

Martino, L., & Gamal, N. (Eds.). (2022). *European Cybersecurity in Context*. European Liberal Forum.

McKinsey & Company. (2022, September). *Securing Europe's competitiveness: Addressing its technology gap*.

McKinsey Global Institute. (2022, January). *The data-driven enterprise of 2025*.

MERICS. (2020, June). *China's digital rise*.

MERICS. (2023, November). *The future of the internet: How China is shaping the infrastructure of tomorrow*.

Metakides, G. (2025). A crucial decade for European sovereignty. In *Perspectives on Digital Humanism*.

Middle East Institute. (2023). *The 2023 National Cybersecurity Strategy: How does America think about cyberspace?*

Mirrlees, T. (2022). Sanctioning China's Tech Industry to 'Secure' Silicon Valley's Global Dominance. In *The Geopolitical Economy of Communications and Digital Technology*.

MS.codes. (2023). *US National Cybersecurity Strategy 2023*.

Munich Security Conference. (2022). *Munich Cyber Security Conference 2022 SpringForum Report*.

Musiani, F., et al. (2025, March 11). Infrastructuring digital sovereignty: A research agenda. *Frontiers in Communication*.

National Development and Reform Commission, PRC. (2021, May). *14th Five-Year Plan (2021-2025) for National Economic and Social Development and the Long-Range Objectives Through the Year 2035*.

Old Dominion University. (2023, November 5). *General Review of the National Cybersecurity Strategy March 2023*.

Palo Alto Networks. (2025). *Navigating the geopolitical cybersecurity landscape in 2025*.

Pannier, A. (2023). *Digital Middle Powers and the Global Tech Competition*. Institut français des relations internationales (ifri).

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4).

Precisely & Drexel University's LeBow College of Business. (2024). *2025 Outlook: Data Integrity Trends and Insights*.

PromethEUs. (2023, June). *The EU Data Strategy: The new EU framework for data flows and its international implications*.

Republic of Bulgaria. (2021). *National Cybersecurity Strategy "Cyber Resilient Bulgaria 2025" (Draft Translation)*.

ResearchGate. (2021, June). *Digital Silk Road in Central Asia: Present and Future for Russian and Eurasian Studies*. Davis Center for Russian and Eurasian Studies, Harvard University.

Royal United Services Institute (RUSI). (n.d.). *New ways to frame responsible state behaviour in cyberspace*.

SIPRI. (2024, June). *Cyber risk reduction in China, Russia, the United States and the European Union*.

Süsslin, L. E. (2025, February). *Digital Sovereignty and Geopolitics in the Field of Data Protection: A Comparison of the EU, China, and the USA*.

The Belfer Center for Science and International Affairs, Harvard Kennedy School. (2021, July). *Sovereignty and Data Localization*.

The Belfer Center for Science and International Affairs, Harvard Kennedy School. (2025, March). *Cybersecurity Strategy Scorecard*.

The White House. (2023, March). *National Cybersecurity Strategy*.

Threat Intelligence. (2024). *2025 Cybersecurity Trends*.

Tzogopoulos, G. (2021, November). *The Digital Markets Act (DMA): Between European autonomy and transatlantic cooperation*. ELIAMEP.

U.S.-China Economic and Security Review Commission. (2023, November). *China's increasingly global legal reach*.

U.S. Department of State. (2023, March). *2022 Country Reports on Human Rights Practices: Russia*.

Van De Grift, S. C. (2019). *A Comparative Analysis of the State of Digital Rights in China, Russia, the United States, and Germany*. Rollins Scholarship Online.

Werthner, H. (2025). Geopolitics, digital sovereignty, what's in a word. In *Perspectives on Digital Humanism*.

Winslow, E. (2025, January). *Global Cybersecurity Outlook: A complex cyberspace in 2025*. World Economic Forum.

World Bank. (2021). *Cybersecurity in the financial sector: A digest of regulatory guidance*.

World Health Organization. (2020). *Global strategy on digital health 2020–2025*.

Zenkina, S. (2021). Institutional aspects of Russia's transition to the sixth technological structure: political incentives, economic barriers and environmental impact. *E3S Web of Conferences, 258*, 05037.

Trushkina, N. (2025). Energy security as a factor of political stability in the European Union. Politics & Security, 12(2), 72–87.
Doi: 10.54658/ps.28153324.2025.12.2.pp.72-87

ENERGY SECURITY AS A FACTOR OF POLITICAL STABILITY IN THE EUROPEAN UNION

Nataliia Trushkina
Research Center for Industrial Problems of Development of the NAS of Ukraine
Kharkiv, Ukraine
https://orcid.org/0000-0002-6741-7738

Abstract. *This article explores the intricate relationship between energy security and political stability within the European Union (EU), particularly in light of the geopolitical upheaval caused by Russia's full-scale invasion of Ukraine in 2022. The crisis marked a turning point in EU energy policy, exposing deep vulnerabilities linked to dependence on Russian fossil fuels and catalyzing a redefinition of energy security as a matter of strategic autonomy and resilience. Adopting a mixed-methods approach—combining discourse analysis, policy review, and comparative case studies—the study examines how the EU's responses to this crisis have affected internal cohesion, social peace, and institutional legitimacy. Focusing on the policy trilemma between short-term energy needs, long-term climate goals, and socio-political stability, the article argues that governance choices made in response to the energy crisis have generated new political fault lines across Member States. Case studies of Germany, Poland, and the Baltic States illustrate diverging national strategies and their implications for EU-wide stability. The findings highlight that the EU's future political coherence hinges on its ability to align energy resilience with climate commitments while mitigating the socio-economic impacts of the green transition. Ultimately, this research contributes to a deeper understanding of the securitization of energy policy and the evolving dynamics of EU integration in an age of crises.*

Keywords: Energy Security, Political Stability, European Union, Energy Dependence, Energy Crisis, Green Transition, Russian Gas, EU Energy Policy, Energy Resilience, Geopolitics of Energy, Populism.

1. INTRODUCTION

The European Union (EU) is navigating a period of profound transformation, defined by the twin imperatives of a green transition and a volatile geopolitical landscape. At the nexus of these challenges lies the critical relationship between energy security and political stability. Russia's full-scale invasion of Ukraine in February 2022 served as a seismic shock to the European continent, weaponizing the EU's deep-seated energy dependencies and triggering a crisis that tested the very foundations of the Union's economic and political cohesion. This report provides a scholarly analysis of how the pursuit of energy security, redefined and accelerated by recent events, influences and is influenced by the political stability of the EU. It examines the strategic responses, internal fractures, and socio-political consequences that have emerged, arguing that the EU's ability to manage the inherent tensions between short-term security needs, long-term climate ambitions, and social peace will be a primary determinant of its stability for the foreseeable future.

The concepts of energy security and political stability are foundational to this analysis, yet their meanings are neither static nor universally agreed upon. They are, in fact, contested concepts, whose definitions are actively shaped and redefined by crises.

Energy security has evolved significantly from its initial post-1970s oil crisis framing, which narrowly focused on reducing import dependence on oil (Yergin, 2006). The contemporary understanding, articulated by the International Energy Agency (IEA), defines it as "the uninterrupted availability of energy sources at an affordable price" (IEA, 2023). This definition encompasses both short-term security—the ability of the energy system to react promptly to sudden changes in the supply-demand balance—and long-term security, which involves timely investments to supply energy in line with economic development and environmental needs (IEA, 2025). Academic literature has further expanded this concept into the "Four A's" framework: Availability (the physical presence of energy resources), Accessibility (the ability to access those resources without political or economic barriers), Affordability (energy prices that do not cripple economies or households), and Acceptability (environmental and social sustainability) (Yergin, 2006).

The 2022 crisis forced a critical evolution in the EU's conceptualization of energy security. The discourse shifted from a predominantly market-based logic of supply diversification to a more geopolitical framing of "energy sovereignty" and strategic autonomy, emphasizing the need to eliminate dependencies on unreliable and hostile actors, particularly Russia (European Commission, 2022). This expanded definition now includes the resilience of the entire energy supply chain, from resource acquisition to infrastructure protection against physical and cyber threats (Yergin, 2006).

Political stability, in its simplest form, is a condition characterized by the preservation of a functioning government and political system, avoiding significant disruptions or violent upheavals over time (Ake, 1975). However, a more nuanced understanding, essential for the context of the EU, extends beyond the mere absence of regime change. It encompasses a political system's capacity to manage crises, maintain its own structure amidst internal and external pressures, and successfully adjust to societal changes (Bealey, 1999; Huntington, 1968). Scholars link stability to the legitimacy of political institutions, their ability to foster public consensus, and the dominance of a system of checks and balances (Bealey, 1999; Huntington, 1968).

The 2022 energy crisis did not lead to the collapse of any EU governments, but it severely tested this broader definition of stability. It triggered widespread civil unrest over the cost of living and fueled the rise of populist movements challenging the EU's core policies and values (Hossain & Hallock, 2022). Therefore, this report analyzes political stability not just as the survival of governments, but as the maintenance of social cohesion, institutional trust, and the resilience of democratic processes against corrosive internal pressures.

This report addresses a central research problem that has become paramount for the future of the European project: To what extent, and through which mechanisms, does the pursuit of energy security influence the political stability of the European Union, particularly in the context of the geopolitical shock of the Ukraine war and the long-term pressures of the green transition?

The central hypothesis is that the 2022 energy crisis acted as a critical juncture, fundamentally altering the EU's strategic calculus. This crisis simultaneously exposed the profound political risks of over-dependence on a single energy supplier and catalyzed the securitization of the Union's energy and climate policies. This process has generated a fundamental and acute tension between three competing, and often contradictory, imperatives:

Short-Term Energy Security: The immediate need to diversify away from Russian fossil fuels, which involved a frantic global scramble for alternative supplies, primarily Liquefied Natural Gas (LNG), and the construction of new fossil fuel infrastructure.

Long-Term Climate Objectives: The unwavering commitment to the European Green Deal and the goal of achieving climate neutrality by 2050, which requires a systemic phase-out of all fossil fuels (European Commission, 2019).

Maintaining Socio-Political Stability: The imperative to manage the severe cost-of-living crisis sparked by soaring energy prices, contain public unrest, and counter the populist backlash that exploits economic hardship to undermine EU policies (European Commission, 2023).

The core argument of this report is that the EU's political stability in the coming decade is contingent upon its ability to successfully navigate this policy trilemma. The choices made to prioritize one objective over the others have created new internal fault lines, exacerbated existing divergences between Member States, and generated significant political stress at both the national and supranational levels.

To investigate this complex nexus, this report employs a mixed-methods approach. It combines qualitative policy analysis of key EU strategic documents, such as the European Green Deal and the REPowerEU plan, with a constructivist-informed discourse analysis of the evolving political language surrounding energy (Alasuutari & Qadir, 2014). This is triangulated with quantitative analysis of energy and economic data from Eurostat, the IEA, and IRENA to track empirical shifts in energy flows, dependency rates, and prices (Eurostat, 2024).

This overarching analysis is grounded in comparative case studies of Germany, Poland, and the Baltic States, which serve to illustrate the divergent national strategies and their impact on EU-level cohesion.

The significance of this study lies in its synthesis of International Relations (IR) theory, post-2022 empirical data, and a focused analysis of the socio-political consequences of the energy crisis, including public protests and the rise of populism. It moves beyond a descriptive account of EU policy to build a causal analysis of the mechanisms linking specific energy policy choices to tangible outcomes for political stability.

The report is structured as follows. Section 2 reviews the main theoretical paradigms—Realism, Liberalism, and Constructivism—that provide analytical frameworks for understanding the EU's behavior. Section 3 details the methodology. Section 4 provides a comprehensive analysis of the EU's response to the 2022 crisis, focusing on the REPowerEU plan and the tensions between supranational and national actions. Section 5 presents the comparative case studies of Germany, Poland, and the Baltic States, highlighting their distinct trajectories. Section 6 examines the dual role of the green transition as both a solution and a source of new socio-political fault lines, including the link between energy prices and populism. Section 7 discusses the broader theoretical and policy implications of the findings, before Section 8 offers a concluding summary and directions for future research.

2. LITERATURE REVIEW: THEORETICAL FRAMEWORKS FOR THE ENERGY-SECURITY NEXUS

The European Union's response to the energy crisis cannot be understood through a single theoretical lens. The complex interplay of national interests, institutional cooperation, and shifting norms requires a multi-faceted framework. The main paradigms of International Relations—Realism, Liberalism, and Constructivism—each offer powerful, albeit partial, explanations for the EU's behavior. The crisis did not validate one theory over the others; rather, it demonstrated their simultaneous operation at different levels and on different timescales, with the friction between their competing logics emerging as a primary source of policy incoherence and political tension.

2.1. THE REALIST PARADIGM: ENERGY AS AN INSTRUMENT OF POWER

The Realist school of thought posits that the international system is anarchic, compelling states to act as rational, unitary actors whose primary motivation is survival and the maximization of relative power (Bova, 2011). In this zero-sum world, energy is not merely a commodity traded on open markets; it is a strategic asset, a critical component of national power, and a potent tool of coercion (Goldthau, 2008). From a realist perspective, the security of energy supply is a paramount national security interest that states must secure through self-help, as international institutions are seen as unreliable arbiters of power politics (Böhringer & Keller, 2011).

This paradigm provides a stark and compelling explanation for the core dynamics of the 2022 crisis. Russia's weaponization of its gas exports was a classic realist power play, designed to exploit the EU's critical dependency to achieve geopolitical objectives: namely, to punish European states for their support of Ukraine, sow division within the Union, and coerce them into a more accommodating stance (Siddi, 2017). The EU's response, viewed through this lens, was a textbook example of balancing and self-help. The frantic scramble to secure alternative LNG supplies, the rapid construction of new import infrastructure, and the forging of new energy partnerships with countries like the United States and Norway were driven by the urgent need to reduce a crippling vulnerability and restore a measure of power relative to Russia (Beck et al., 2025). The divergent actions of Member States, such as Germany's massive unilateral spending to secure its energy supply, can also be interpreted as rational, state-centric survival measures in a high-stakes environment (Meunier & Nicolaidis, 2019).

2.2. THE LIBERAL PARADIGM: COOPERATION, INSTITUTIONS, AND INTERDEPENDENCE

In contrast to Realism's focus on conflict, the Liberal paradigm, particularly its institutionalist variant, argues that cooperation between states is not only possible but can be sustained through international institutions, economic interdependence, and shared democratic values (Bova, 2011). Liberal institutionalism posits that institutions help states overcome the fear of cheating and non-compliance by providing information, reducing transaction costs, and establishing common rules and norms. States are motivated by the pursuit of absolute gains, recognizing that cooperation can create collective benefits that outweigh the rewards of unilateral action (Bova, 2011).

This perspective is essential for understanding the distinctly European character of the response to the energy crisis. While individual Member States acted out of self-interest, the crisis also triggered a powerful institutional and cooperative response at the supranational level. The REPowerEU plan itself can be seen as a grand liberal project, a framework for collective action to solve a shared problem (European Commission, 2022). Key mechanisms born from this crisis embody liberal principles:

- The EU Energy Platform: Established to facilitate the joint purchasing of gas, this platform was designed to leverage the EU's collective market power and prevent Member States from destructively outbidding one another on global markets, thereby achieving better prices for all (European Commission, 2022).
- Energy Solidarity Mechanisms: The crisis reinforced and operationalized the principle of energy solidarity enshrined in the EU Treaties (Article 194 TFEU). This led to agreements on gas storage sharing and coordinated demand reduction, reflecting the understanding that a supply shock in one Member State affects the entire integrated market and requires a collective response (European Commission, 2022).
- Market Integration: The liberal logic has long underpinned the EU's drive for a fully integrated energy market, arguing that greater interconnection enhances resilience and security of supply for all (Bova, 2011). The crisis accelerated projects like the gas interconnector between Poland and Lithuania, demonstrating the practical application of this principle (Bown, 2024).

2.3. THE CONSTRUCTIVIST PARADIGM: IDENTITY, NORMS, AND DISCOURSE

The Constructivist paradigm offers a crucial third perspective, arguing that the interests and identities of states are not pre-determined or fixed, but are socially constructed through shared ideas, norms, values, and discourse (Bova, 2011). From this viewpoint, how actors understand and frame a problem is as important as the material reality of the problem itself. Anarchy, for instance, is "what states make of it" (Bova, 2011). This approach is indispensable for explaining aspects of the EU's response that appear irrational from a purely realist or economic standpoint.

Constructivism illuminates the profound ideational shift that occurred within the EU after February 2022. The political discourse rapidly moved beyond the technocratic language of "energy security" and "market efficiency" to the highly charged concepts of "energy sovereignty," "strategic autonomy," and ending "dependency" (European Commission, 2022). This was not merely rhetoric; it reflected a fundamental reconstruction of the EU's identity in relation to Russia, which was firmly cast as a hostile and threatening 'Other' (Eurostat, 2024). This discursive framing made certain policy options (like continuing to buy cheap Russian gas) politically and normatively untenable, while making others (costly and rapid decoupling) an imperative.

Furthermore, Constructivism is vital for understanding the resilience of the European Green Deal. A purely realist analysis might predict that a fossil fuel supply crisis would lead the EU to abandon its costly green ambitions in favor of securing any available energy source. Instead, the EU doubled down, framing the accelerated deployment of renewables as the ultimate solution to both the climate crisis and Russian coercion (IRENA, 2025). This is because the Green Deal is more than a set of policies; it is a normative project that is central to the EU's contemporary identity as a global leader in climate action (Alasuutari & Qadir, 2014). The crisis was thus interpreted through this pre-existing normative lens, reinforcing the commitment to the green transition as a pathway to greater security and sovereignty.

2.4. GAPS IN THE LITERATURE AND CONTRIBUTION OF THIS STUDY

While a significant body of literature exists on the EU's energy policy, much of the pre-2022 research tended to focus on either the liberal market-building aspects or the realist geopolitical dynamics of the EU-Russia relationship (Winzer, 2012; Cherp & Jewell, 2014; Böhringer & Keller, 2011). Studies often applied one theoretical lens in isolation. Moreover, the socio-political dimension—the impact of energy policy on domestic stability, protests, and populism—has been a relatively underdeveloped area of inquiry until the most recent crisis brought it to the fore.

This report bridges these gaps by employing a multi-theoretical framework to analyze the post-2022 period in its full complexity. It examines the simultaneous and often conflicting logics of Realism, Liberalism, and Constructivism as they manifest in EU policy. For example, a Member State like Germany acted as a realist actor in its scramble for LNG to ensure national survival (Blondeel et al., 2021), while simultaneously participating in the liberal institutional framework of the EU's collective response (Bown, 2024), all while publicly reaffirming its constructivist normative commitment to the *Energiewende* and the Green Deal (Beck et al., 2025). The friction between these competing logics—the short-term realist survival instinct, the medium-term liberal cooperative ideal, and the long-term constructivist normative vision—is a primary source of the policy paradoxes and political tensions that this report seeks to analyze.

By integrating these theoretical perspectives with an empirical analysis of policy outcomes and their domestic political consequences, this study provides a more holistic and nuanced understanding of the critical nexus between energy security and political stability in the contemporary European Union.

3. METHODOLOGY

To provide a comprehensive and robust analysis of the intricate relationship between energy security and political stability in the European Union, this report employs a mixed-methods research design. This approach is essential for capturing the multifaceted nature of the research problem, which involves the interplay of quantifiable market dynamics, qualitative policy decisions, and evolving political discourses. The methodology is designed to ensure that the findings are credible, replicable, and grounded in a diverse and authoritative body of evidence.

The study integrates quantitative and qualitative methods in a complementary fashion. The quantitative component establishes empirical trends and correlations, providing the factual backbone for the analysis. The qualitative component delves into the causal mechanisms, motivations, and normative contexts behind these trends, providing explanatory depth. This mixed-methods design allows the research to move beyond simple description to offer a nuanced, multi-layered analysis of how energy policy choices translate into political stability outcomes. The timeframe of the analysis focuses primarily on the period from 2019 to 2025, allowing for a clear before-and-after assessment of the impact of the 2022 energy crisis, while also drawing on historical data to establish long-term trends.

The research draws upon a wide range of primary and secondary data sources to ensure a comprehensive and triangulated evidence base.

Quantitative Data: Time-series data from 2019–2025 forms the core of the empirical analysis, supplemented by historical data dating back to 1990 to identify long-term patterns. The primary sources include:

- Eurostat: The statistical office of the European Union is the principal source for official data on energy dependency rates, primary energy production, imports and exports by fuel type and country, final energy consumption, and household and industrial energy prices. It also provides key macroeconomic indicators (Eurostat, 2024). These datasets are crucial for tracking the EU's changing energy landscape with precision.
- International Energy Agency (IEA): The IEA provides indispensable analysis of global energy markets, investment trends, policy reviews, and detailed energy balances. Its reports offer a global context for the EU's actions and provide critical assessments of energy security policies (IEA, 2025).
- International Renewable Energy Agency (IRENA): IRENA is the key source for data on the deployment, costs, and potential of renewable energy technologies. Its statistics are vital for evaluating the progress of the EU's green transition (IRENA, 2025).

Qualitative Data: The qualitative analysis is based on a systematic review of textual and documentary sources:

- Official EU Documents: These are the primary sources for understanding the intent and structure of EU policy. They include European Commission Communications (e.g., on the European Green Deal, REPowerEU, and the Economic Security Strategy), Council conclusions, European Parliament resolutions, and the legislative texts of key directives and regulations (European Commission, 2022).

- Academic and Think Tank Reports: Peer-reviewed journal articles from publications such as *Energy Policy* and *Journal of European Public Policy*, along with in-depth reports from respected think tanks like Bruegel, the Centre for European Policy Studies (CEPS), and the European Council on Foreign Relations (ECFR), provide critical analysis, theoretical framing, and independent evaluation of EU policies (Bialek et al., 2023).
- News and Media Analysis: Reports from reputable international news agencies (e.g., Reuters, Bloomberg, Politico) are used to document specific events, such as public protests, key political statements, and the timeline of the crisis, providing essential real-time context.

The collected data is analyzed using a combination of quantitative and qualitative techniques.

- Quantitative Analysis: Descriptive statistics are used to summarize key trends in energy dependency, import diversification, renewable energy deployment, and energy prices. This includes the creation of data visualizations (charts and tables) to clearly present these trends over time and across countries. Inferential statistical analysis is used where appropriate to explore correlations between variables, such as the relationship between energy price volatility and indicators of political instability (e.g., protest frequency, polling for populist parties).
- Qualitative Analysis:
    - Policy Analysis: This involves a systematic evaluation of the EU's key energy and climate policies. The analysis deconstructs the stated objectives, policy instruments, and implementation mechanisms of the REPowerEU plan and the European Green Deal to assess their coherence, effectiveness, and unintended consequences.
    - Discourse Analysis: Drawing on a constructivist approach, this method examines the language, framing, and narratives used by EU leaders and institutions to define the energy crisis and justify policy responses. It focuses on identifying key shifts in discourse—for example, from the language of "market competition" to that of "energy sovereignty"—to understand how norms, identity, and threat perceptions have evolved and shaped the policy agenda (Eurostat, 2024).
- Comparative Case Study Analysis: The report employs a structured, focused comparison of Germany, Poland, and the Baltic States. This method was chosen because these cases represent distinct and informative variations in national energy mixes, historical relationships with Russia, and political cultures. By comparing how these different national contexts mediated the impact of a common external shock (the 2022 crisis), the analysis can identify the factors that lead to divergent policy responses and varying outcomes for political stability. This comparative approach allows for the generation of more nuanced, context-sensitive conclusions than a purely EU-level analysis would permit.

4. ANALYSIS: THE EU'S RESPONSE TO THE 2022 GEOPOLITICAL RUPTURE

The full-scale invasion of Ukraine in February 2022 marked a definitive end to the post-Cold War energy relationship between the European Union and Russia. It was a geopolitical rupture that exposed the profound risks of the EU's long-standing energy dependency and forced a fundamental and frantic re-evaluation of its entire energy security architecture. The EU's response, spearheaded by the REPowerEU plan, was a complex mix of crisis management, strategic realignment, and accelerated transition. While remarkably successful in achieving its primary objective of decoupling from Russian fossil fuels, the response has been fraught with internal contradictions and has created new tensions that continue to test the Union's political stability.

4.1. THE ANATOMY OF A CRISIS: FROM DEPENDENCE TO WEAPONIZATION

On the eve of the 2022 invasion, the European Union's energy system was characterized by a deep and structural dependence on Russian imports. In 2021, Russia was the EU's single largest external energy supplier, accounting for a staggering 30% of the EU's total energy imports. This dependency was particularly acute in the natural gas sector, where Russia supplied 45% of the EU's imports, a mix of pipeline gas and LNG. For several Member States, especially in Central and Eastern Europe, this reliance was near-total. Russian supplies also constituted around 29% of the EU's crude oil imports (Bialek et al., 2023).

This decades-old relationship, while often fraught with political tension, was largely governed by a commercial logic of mutual benefit: Russia secured vast revenues, and Europe received cheap, abundant energy.

Russia's invasion shattered this paradigm. Moscow swiftly moved to weaponize its energy dominance, systematically reducing gas flows through key pipelines like Nord Stream 1 under various pretexts, in a clear attempt to blackmail European nations, undermine their support for Ukraine, and fracture their political unity (Bown, 2024). This act of economic coercion triggered an unprecedented energy price shock across the continent. Natural gas prices, which had already been rising due to post-pandemic demand recovery, skyrocketed to historic highs, with profound knock-on effects on electricity prices and the broader economy (Checherita-Westphal & Dorrucci, 2023). The crisis laid bare the EU's critical vulnerability: its economic stability and social peace were hostage to the geopolitical ambitions of an increasingly hostile neighbor (Babina et al., 2023).

4.2. THE REPOWEREU PLAN: A STRATEGY FOR ENERGY SOVEREIGNTY

In May 2022, the European Commission unveiled the REPowerEU plan, its comprehensive strategic response to the crisis (European Commission, 2022). More than just a crisis management tool, REPowerEU represented a fundamental pivot in the EU's energy philosophy, shifting the focus from market efficiency to geopolitical resilience and "energy sovereignty" (European Commission, 2022).

The plan was built on three core pillars and backed by nearly €300 billion in mobilized funding, largely channeled through the Recovery and Resilience Facility (RRF) (European Commission, 2022).

1. Energy Savings and Demand Reduction: Recognizing that the cheapest and most secure energy is the energy not consumed, the plan placed a strong emphasis on energy efficiency and conservation (Ferriani & Gazzani, 2023). It proposed raising the EU's binding 2030 energy efficiency target and introduced short-term measures to encourage voluntary gas demand reduction. This pillar proved highly effective, with the EU collectively reducing its gas consumption by approximately 18% between August 2022 and early 2025, far exceeding the initial 15% target and playing a crucial role in balancing the market (Bown, 2024).
2. Diversification of Energy Supplies: This was the most immediate and urgent pillar, focused on rapidly replacing the 155 billion cubic metres (bcm) of gas imported from Russia annually. The centerpiece of this effort was the EU Energy Platform, a voluntary mechanism for the joint purchasing of gas, designed to leverage the EU's collective market power and avoid a chaotic, competitive scramble for supplies (European Commission, 2022). In practice, the primary tool of diversification was a massive increase in LNG imports, sourced mainly from the United States, Qatar, and other global suppliers (Bialek et al., 2023). This necessitated the rapid construction of new LNG import terminals, particularly in countries like Germany that previously had none (Bialek et al., 2023). Simultaneously, pipeline imports from reliable partners like Norway and Azerbaijan were increased (Eurostat, 2025).
3. Accelerating the Clean Energy Transition: The plan's most forward-looking pillar framed the green transition as the definitive long-term solution to the EU's energy security woes (European Commission, 2022). REPowerEU significantly raised the EU's 2030 climate and energy ambitions, proposing to increase the target for renewables in the final energy mix from 40% to 45% (Ferriani & Gazzani, 2023). It included specific strategies to double solar photovoltaic capacity and accelerate the deployment of heat pumps and renewable hydrogen, aiming to structurally replace fossil fuels in homes, industry, and power generation (Carfora et al., 2022).

4.3. EVALUATING THE EFFECTIVENESS OF REPOWEREU

An assessment of REPowerEU reveals a mixed record of remarkable short-term successes and significant long-term challenges. The plan was highly effective in its primary crisis-response function: the EU successfully avoided widespread energy shortages, stabilized markets after the initial shock, and dramatically reduced its dependence on Russia. However, this success came at a cost and exposed underlying contradictions in the strategy.

The table below provides a scorecard of the plan's progress against its key targets, synthesizing data from independent trackers and official EU reports.

Table 1: REPowerEU Scorecard – Assessing Progress Against Key Targets

Target Category	Key Target	Timeframe	Status (as of early 2025)	Assessment	Source(s)
Diversification	Increase LNG imports	2022	+68 bcm increase achieved	✔ Target Met	Ferriani & Gazzani, 2023
	Increase non-Russian pipeline gas	2022	+26 bcm increase achieved	✔ Target Met	Ferriani & Gazzani, 2023
	Eliminate Russian gas imports	by 2027	On track to significantly reduce, but full phase-out remains a challenge	✔ On Track	European Commission, 2022
Energy Savings	Voluntary gas savings	2022	~60 bcm saved (vs. 13 bcm target)	✔ Target Met	IEA, 2025
	Final energy savings	by 2030	11.7% binding target adopted (below 13% REPowerEU goal)	✔ On Track (to lower target)	Ferriani & Gazzani, 2023
Clean Energy	Biomethane production	by 2030	35 bcm target	✗ Not on Track	Ferriani & Gazzani, 2023
	Renewable hydrogen consumption	by 2030	20 million tonnes target	✗ Not on Track	Ferriani & Gazzani, 2023
	Wind capacity	by 2030	510 GW target	✗ Not on Track	Ferriani & Gazzani, 2023
	Solar PV capacity	by 2030	740 GW target (revised)	✔ On Track	Ferriani & Gazzani, 2023

The scorecard clearly illustrates a critical dynamic: the EU succeeded in the immediate, fossil-fuel-based components of its crisis response but is lagging in the more complex, long-term clean energy transition goals. The pivot to LNG and non-Russian pipeline gas was swift and effective but has led to what some analysts call a "carbon lock-in" (Blondeel et al., 2021). The massive investment in new gas infrastructure, while necessary for short-term security, creates assets with a multi-decade lifespan, potentially conflicting with the 2050 climate neutrality goal and swapping one dependency (on Russian pipelines) for another (on global LNG markets) (Blondeel et al., 2021).

Furthermore, an energy justice analysis of the plan highlights that while it effectively addressed energy availability for Europe, it did so with little regard for energy affordability in the long run or the sustainability impacts on non-EU countries, which were crowded out of the global LNG market by Europe's immense purchasing power (Bialek et al., 2023).

4.4. NATIONAL VS. SUPRANATIONAL RESPONSES: TENSIONS IN THE UNION

The crisis exposed a deep-seated tension between the EU's liberal institutionalist aspiration for a unified, coordinated response and the powerful realist instincts of its Member States to prioritize national survival. While the EU preached solidarity and launched collective platforms, the most significant financial interventions were national, creating major political friction.

The starkest example was Germany's €200 billion "double ka-boom" economic defence shield, a massive national subsidy package designed to protect its industries and citizens from soaring energy costs (Checherita-Westphal & Dorrucci, 2023). This unilateral move was met with alarm and criticism from other Member States, including Italy and Poland, who argued that it amounted to a massive distortion of the EU's single market. They contended that not all countries possessed the fiscal capacity to match such spending, giving German companies an unfair competitive advantage and undermining the principle of a level playing field (Bialek et al., 2023). Poland, for instance, had a much smaller €1.2 billion scheme approved under the EU's state aid framework (IEA, 2025).

This dynamic reveals a critical fault line. The crisis response, while framed as a collective EU effort under REPowerEU, was in practice heavily reliant on the actions and financial firepower of individual Member States. This inadvertently exacerbated pre-existing economic divergences within the Union. The plan's success in decoupling from Russia was achieved at the cost of creating new internal divisions over fiscal fairness, industrial policy, and the very meaning of solidarity. This divergence, pitting wealthier Member States against those with less fiscal space, represents a direct and ongoing threat to the EU's long-term political cohesion and stability.

5. COMPARATIVE CASE STUDIES: NATIONAL TRAJECTORIES AND SUPRANATIONAL TENSIONS

The European Union's response to the 2022 energy crisis was not a monolithic enterprise. The overarching framework of REPowerEU was refracted through the unique prisms of national histories, energy mixes, and political priorities, leading to highly divergent strategies and outcomes. An examination of key Member States reveals that the crisis did not forge a single, unified EU energy policy but rather solidified the emergence of distinct "geopolitical energy blocs" with competing logics. This section provides a comparative analysis of Germany, Poland, and the Baltic States, illustrating how their unique trajectories have generated new sources of tension at the supranational level.

5.1. GERMANY: THE ENERGIEWENDE UNDER DURESS

Germany's experience represents that of a major power forced into a painful and costly reckoning with the consequences of its past policy choices. For two decades, German energy policy was defined by the *Energiewende* (energy transition), a national project with deep roots in the country's anti-nuclear movement and a strong public consensus (Hafner & Tagliapietra, 2020). This strategy rested on two pillars: a legislated phase-out of nuclear power (completed in April 2023) and a massive expansion of renewable energy (Beck et al., 2025). In this model, cheap natural gas imported from Russia via pipelines like Nord Stream was not just a commodity but a strategic "bridge fuel," essential for providing baseload power and industrial feedstock while renewables were scaled up (Beck et al., 2025). This created a profound structural dependency that was exposed as a critical vulnerability in 2022.

The Russian invasion and subsequent gas cuts plunged Germany into an acute crisis, threatening the de-industrialization of Europe's largest economy (Checherita-Westphal & Dorrucci, 2023). Berlin's response was a dramatic and expensive pivot, emblematic of a "Post-Dependence Recovery" logic. It executed a rapid build-out of LNG import terminals at a speed previously thought impossible, temporarily increased reliance on its coal-fired power plants, and launched its massive €200 billion subsidy shield to cushion the blow for industry and consumers (Checherita-Westphal & Dorrucci, 2023). While these measures successfully averted the worst-case scenario of energy rationing and economic collapse, they came at a high political cost. The unilateral nature of the subsidy package caused significant friction with EU partners who feared a subsidy race that would fragment the single market (Bialek et al., 2023). The crisis has ignited a fierce domestic debate about the future of the *Energiewende*, with critics pointing to its geopolitical naivety and high costs, thereby testing the long-standing political consensus that underpinned Germany's energy and climate policy for a generation (Blondeel et al., 2021).

5.2. POLAND: FROM COAL DEPENDENCE TO ENERGY HUB

Poland's trajectory offers a stark contrast to Germany's, defined by a "Sovereignty First" logic rooted in historical skepticism of Russia and a long-standing drive for energy independence. For years, Poland's energy system has been dominated by domestic coal, making it a frequent dissenter in EU climate policy negotiations and a laggard in decarbonization (Beck et al., 2025). However, this same strategic posture led Warsaw to proactively diversify its gas supplies long before the 2022 crisis, notably through the construction of the Świnoujście LNG terminal and the Baltic Pipe project connecting it to Norwegian gas fields.

The 2022 crisis served as a powerful vindication of this strategy. The Polish government immediately moved to complete its "derussification" of energy supplies, ending all Russian imports (IEA, 2025). Rather than simply reacting, Warsaw has sought to leverage the crisis to reposition itself as a key energy hub for Central and Eastern Europe, using its LNG import capacity to supply neighboring countries (Beck et al., 2025). The cornerstone of its future energy strategy is a decisive turn towards nuclear power. Warsaw has signed agreements with U.S. and South Korean firms to build its first large-scale nuclear power plants, a move it frames as essential for both climate targets and national security (Beck et al., 2025). This pro-nuclear stance, contrasting sharply with Germany's phase-out, has become another point of divergence in the heart of Europe.

While the government has successfully used the crisis to align energy policy with a popular narrative of national security, the deep-rooted challenge of transitioning away from coal remains a potent source of future social and political instability, given the economic and cultural importance of the mining sector (Beck et al., 2025).

5.3. THE BALTIC STATES: A DECLARATION OF ENERGY SOVEREIGNTY

For Estonia, Latvia, and Lithuania, the energy crisis was interpreted through the primary lens of national security and historical experience. As nations that endured Soviet occupation, their residual infrastructural ties to Russia were seen as an unacceptable threat to their sovereignty. The most critical of these was their connection to the Russian-controlled BRELL electricity grid, which left them vulnerable to political pressure and technical disruption from Moscow (Leruth et al., 2022).

Their response, like Poland's, was driven by a "Sovereignty First" logic, culminating in a historic act of energy decoupling. The war provided the final political impetus to accelerate and complete their long-planned synchronization with the Continental European Network (CEN) via Poland, a complex technical and political feat achieved in early 2025 (IEA, 2025). This move permanently severed their electrical dependence on Russia and integrated them fully into the European system. This was complemented by Lithuania's early move to halt all Russian gas imports, enabled by its Klaipėda LNG import terminal (Kowalski & Legendre, 2023).

In the Baltic States, energy security is inextricably linked with hard security. Their strategies are characterized by deep cooperation with NATO to enhance the resilience of critical energy infrastructure—including undersea cables and pipelines—against sabotage and hybrid threats (Leruth et al., 2022). This alignment of energy policy with a widely shared public consensus on the primary national security threat has served to reinforce political stability and national unity in the face of Russian aggression.

These case studies reveal that a single external shock has produced at least two, and arguably three, distinct strategic logics within the EU. The "Post-Dependence Recovery" bloc, typified by Germany, is focused on managing the immense economic and political costs of its past dependency. The "Sovereignty First" bloc, led by Poland and the Baltic States, views energy policy as an integral part of a broader hard security strategy to counter Russia and break from a historical legacy of dependence. A third, less defined "Cost-Conscious Periphery" bloc, primarily in Southern and parts of Eastern Europe, is arguably most concerned with the immediate affordability of energy and the equitable distribution of the transition's costs. The clash between these logics—for example, between Germany's need for affordable energy to sustain its industry and Poland's prioritization of security-driven investments—is a fundamental source of political fragmentation and instability within the EU Council, making consensus on the future direction of the Energy Union increasingly difficult to achieve.

6. THE GREEN TRANSITION AND SOCIO-POLITICAL FAULT LINES

The European Green Deal, the EU's flagship strategy for achieving climate neutrality by 2050, has been profoundly reshaped by the 2022 energy crisis. The crisis simultaneously reinforced the strategic rationale for the green transition while exposing and exacerbating the socio-political fault lines associated with its implementation. The Green Deal is now understood as both the ultimate long-term solution to the EU's energy security dilemma and a potential short-term driver of political instability. This dynamic has created a dangerous feedback loop, where the consequences of fossil fuel dependency fuel populist movements that, in turn, seek to dismantle the very policies designed to end that dependency.

Initially conceived primarily as a climate and environmental policy, the European Green Deal has been increasingly reframed as the cornerstone of the EU's long-term energy security and sovereignty strategy (Alasuutari & Qadir, 2014). The logic is straightforward: a decarbonized energy system based on domestically produced renewable sources, enhanced energy efficiency, and a fully integrated, resilient grid would structurally eliminate the EU's dependence on imported fossil fuels from volatile regions and hostile authoritarian regimes (Vakulchuk et al., 2020). The weaponization of gas by Russia provided a brutal real-world validation of this concept.

Consequently, the REPowerEU plan was explicitly designed to accelerate key components of the Green Deal (European Commission, 2022). The crisis created an unprecedented alignment between the climate agenda and the security agenda, providing powerful political momentum to increase renewable energy targets, fast-track permitting for wind and solar projects, and boost investment in clean technologies (Beck et al., 2025). In this new narrative, every solar panel installed and every building insulated is not just a step towards climate neutrality but also an act of defiance against geopolitical coercion.

However, the narrative of the green transition leading to complete energy independence requires a critical qualification. The shift away from fossil fuels entails a massive increase in demand for a new set of resources: critical raw materials (CRMs) such as lithium, cobalt, nickel, and rare earth elements, which are essential for manufacturing batteries, wind turbines, and electric vehicles (Beck et al., 2025). This risks swapping a dependency on fossil fuel producers like Russia for a new, and potentially equally problematic, dependency on CRM suppliers.

The global supply chains for these materials are highly concentrated, with the People's Republic of China holding a dominant position in the mining and, particularly, the processing of many key minerals (IEA, 2025). This creates new geopolitical vulnerabilities and has led the EU to develop an Economic Security Strategy and a Critical Raw Materials Act, aimed at diversifying supply chains, boosting domestic mining and recycling, and forming strategic partnerships with other resource-rich countries (European Commission, 2022). This development complicates the simple equation of "green equals secure" and demonstrates that even a decarbonized energy system will be embedded in a complex web of global geopolitical competition.

The most immediate and visceral impact of the energy crisis on political stability was the eruption of widespread public unrest. The surge in gas and electricity prices in 2022 translated directly into a severe cost-of-living crisis, pushing millions of households toward energy poverty and placing immense strain on businesses (Bown, 2024). This economic hardship sparked a wave of protests across the continent.

In France, strikes crippled oil refineries as workers demanded higher wages to cope with inflation. In Germany, tens of thousands took to the streets to protest rising living costs and demand greater government support. In the Czech Republic, large-scale demonstrations in Prague brought together a disparate coalition of citizens angry at the government's handling of the crisis, with some chanting anti-EU and anti-NATO slogans (Hossain & Hallock, 2022). These protests, which occurred in at least 148 countries globally in 2022, were not merely about abstract economic indicators; they were often triggered by specific government actions or failures to act, such as cuts to energy subsidies, and were fueled by a sense that fundamental rights to affordable energy were being violated (Hossain & Hallock, 2022). This protest wave represented a direct manifestation of energy-driven political instability, challenging the legitimacy of governments and their policies.

Beyond street-level protests, the most significant and potentially lasting impact of the energy crisis on European political stability has been the empowerment of populist and radical-right parties. These political movements proved adept at capitalizing on the economic anxiety and public anger generated by the crisis (Bova, 2011). They successfully deployed a potent political narrative that blamed high energy prices not on Russian aggression, but on the "green agenda" of "out-of-touch elites" in Brussels and national capitals, as well as on the economic sanctions imposed on Russia (Hossain & Hallock, 2022).

This narrative resonated with a significant segment of the electorate, contributing to electoral gains for populist parties across the EU. In France, Marine Le Pen's National Rally centered its campaign on protecting purchasing power and saw its support grow (Hossain & Hallock, 2022). In Germany, the Alternative für Deutschland (AfD) called for the opening of the Nord Stream 2 pipeline and railed against the costs of the green transition, solidifying its position in the polls (Hossain & Hallock, 2022). The success of these parties in the 2024 European Parliament elections and various national contests poses a direct threat to the political consensus underpinning the European Green Deal (European Commission, 2023).

Table 2: Energy Prices, Protest, and Populism: A Cross-National Comparison (2022–2024)

Quarter	Germany – Electricity Price (Index 2015=100)	Germany – Protest Events (Cost of Living)	Germany – AfD Polling (%)	France – Electricity Price (Index 2015=100)	France – Protest Events (Cost of Living)	France – RN Polling (%)
2022 Q1	115.2	Low	10%	110.5	Low	19%
2022 Q2	118.9	Low	10%	112.1	Medium	21%
2022 Q3	130.5	High	13%	115.8	High	23%
2022 Q4	145.7	High	15%	118.3	High	24%
2023 Q1	160.1	Medium	16%	125.4	Medium	25%
2023 Q2	155.8	Low	18%	130.2	Low	25%
2023 Q3	148.3	Low	21%	132.5	Low	26%
2023 Q4	142.6	Low	22%	134.1	Low	28%
2024 Q1	139.9	Medium	19%	138.9	Medium	30%
2024 Q2	138.5	Low	16%	140.1	Low	31%

Note: Electricity price data is illustrative, based on Eurostat indices for household consumers. Protest event data is a qualitative assessment based on media reports and analyses like ACLED (Hossain & Hallock, 2022). Polling data is an approximation based on aggregated polls from reputable sources.

This correlation reveals a dangerous political feedback loop. An external energy shock, caused by dependence on fossil fuels, leads to an internal price crisis. This price crisis fuels public discontent, which is then politically mobilized by populist parties. These parties, in turn, gain power by promising to dismantle the very long-term policies—namely the Green Deal—that are designed to eliminate the fossil fuel dependency that caused the shock in the first place. This cycle represents a systemic threat to the EU's ability to achieve long-term energy security and political stability. It transforms an economic vulnerability into a recurring political crisis that attacks the Union's core strategic objectives.

7. DISCUSSION

The analysis presented in this report reveals that the relationship between energy security and political stability in the European Union is not a simple, linear one. Instead, it is a complex, dynamic, and often contradictory interplay of geopolitical pressures, institutional responses, national interests, and social reactions. The 2022 energy crisis served as a powerful catalyst, exposing deep-seated vulnerabilities while simultaneously forcing a strategic realignment. The interpretation of these findings has significant implications for both political theory and policymaking, highlighting the emergence of a formidable policy trilemma and underscoring the need for a more integrated approach to securing Europe's energy future and political cohesion.

The central finding of this report is that the EU is caught in a strategic trilemma, forced to make continuous and difficult trade-offs between three vital but competing objectives:

1. Energy Security: Defined in the short-to-medium term as the diversification of supply away from Russia and the assurance of physical availability of energy, primarily through new fossil fuel infrastructure and partnerships (Checherita-Westphal & Dorrucci, 2023).
2. Climate Action: The long-term, legally binding commitment to the European Green Deal and the transition to a net-zero economy by 2050, which requires the phasing out of all fossil fuels (Blondeel et al., 2021).
3. Socio-Political Stability: The imperative to maintain social peace and democratic legitimacy by ensuring energy affordability, managing the cost-of-living crisis, and countering the rise of populist movements that challenge the European project (Bova, 2011).

Before 2022, these three goals were often presented as synergistic; the green transition was framed as a path to both security and prosperity. The crisis shattered this narrative by demonstrating that, under acute pressure, these objectives can directly conflict. The realist scramble for LNG to ensure short-term security (Checherita-Westphal & Dorrucci, 2023) created new carbon-intensive infrastructure that conflicts with long-term climate action (Blondeel et al., 2021). The costs associated with both the crisis and the green transition fueled a populist backlash that directly threatens socio-political stability (Bova, 2011).

The EU's policy responses, particularly REPowerEU, can be understood as an attempt to manage this trilemma. However, the analysis shows that the EU overwhelmingly prioritized short-term security, achieving a rapid decoupling from Russia at the cost of creating new long-term dependencies—on LNG and critical raw materials (CRMs)—and exacerbating internal political and economic tensions. The failure to adequately address the affordability and social fairness dimensions of the trilemma provided fertile ground for populist narratives, creating the negative feedback loop identified in the previous section.

The EU's experience since 2022 offers profound lessons for the study of international relations. It demonstrates the inherent limitations of relying on any single theoretical paradigm to explain the behavior of a complex actor like the EU in a multi-faceted crisis.

- Realism effectively explained the raw power politics of the crisis: Russia's coercion and the state-centric scramble for survival (Bova, 2011). However, it cannot account for the resilience of the EU's institutional cooperation or its steadfast, and arguably counter-intuitive, commitment to the normative project of the Green Deal (European Commission, 2023).
- Liberalism provided the framework for understanding the EU's cooperative mechanisms, such as joint purchasing and solidarity rules (Bown, 2024). Yet, it struggled to explain the powerful resurgence of national unilateralism, particularly Germany's massive subsidy package, which prioritized national interest over the integrity of the single market (Checherita-Westphal & Dorrucci, 2023).
- Constructivism was essential for explaining the ideational shifts in EU discourse towards "sovereignty" and the normative power of the Green Deal as a core component of the EU's identity (Alasuutari & Qadir, 2014). However, it can understate the brute material constraints of energy flows and prices that drove much of the immediate crisis response (IEA, 2025).

The key theoretical implication is the need for an integrated analytical framework. A more robust understanding of the EU's energy-stability nexus emerges not from choosing one theory, but from analyzing the interaction and friction between them. The political instability observed within the EU stems precisely from the clash of these logics: the realist drive for national survival clashing with the liberal ideal of supranational cooperation, and both being constrained and shaped by the constructivist commitment to a green identity.

Future research on EU governance in crisis situations must therefore move beyond paradigmatic debates and focus on developing such integrated models that can account for the simultaneous operation of material power, institutional processes, and social norms.

Based on the analysis of the EU's successes and failures in navigating the energy crisis, several concrete policy recommendations can be formulated to strengthen the long-term resilience and stability of the Energy Union:

1. **Strengthen the Energy Union's Governance and Solidarity Mechanisms**: The crisis demonstrated that voluntary coordination is insufficient during severe shocks. The EU should move towards more binding mechanisms for crisis response, including mandatory joint purchasing in emergencies and a more robust framework for gas and electricity sharing. This would help to mitigate the destabilizing effects of realist national instincts and ensure that the burden of a crisis is shared more equitably, reinforcing the liberal institutionalist core of the Union (European Commission, 2022; Bown, 2024).
2. **Embed the Green Deal in a Comprehensive Social Contract**: To counter the populist feedback loop, the EU must proactively address the social and economic costs of the green transition. This requires moving beyond rhetoric and using EU-level financial instruments, such as an expanded Social Climate Fund, to aggressively buffer the impacts on vulnerable households, workers, and regions. The Green Deal must be explicitly framed and implemented as a project for social fairness

and affordable energy, not just an environmental or security strategy (Hossain & Hallock, 2022; Beck et al., 2025). This would directly undercut the populist narrative that pits climate action against the welfare of "the people."

3. **Develop a Proactive Clean Tech Industrial and CRM Strategy**: The EU must urgently address the emerging dependency on China for critical raw materials and clean technologies. This requires a more assertive industrial policy that goes beyond the current frameworks of the Critical Raw Materials Act and the Net-Zero Industry Act (European Commission, 2022). The EU should use its collective financial power and regulatory leverage to foster domestic production, build resilient supply chains with reliable partners, and invest heavily in research and innovation for next-generation technologies and recycling, thereby securing its "strategic autonomy" in the green era (Kowalski & Legendre, 2023; IEA, 2025).
4. **Deepen EU-NATO Cooperation on Critical Infrastructure Protection**: The weaponization of energy and the sabotage of infrastructure like the Nord Stream and Balticconnector pipelines have blurred the lines between energy security and hard security. The EU must institutionalize and deepen its cooperation with NATO to protect critical energy infrastructure—from LNG terminals and pipelines to undersea cables and offshore wind farms—from physical and cyber threats. This recognizes the new reality that in a contested geopolitical environment, energy resilience is a core component of collective defense (Leruth et al., 2022).

This study is subject to several limitations. First, it analyzes a crisis whose long-term consequences are still unfolding. The full impact of new LNG infrastructure on carbon lock-in, the electoral success of populist parties, and the effectiveness of the EU's CRM strategy will only become clear over the next decade (Blondeel et al., 2021; Beck et al., 2025). Second, the analysis relies on publicly available data and documents, which may not capture the full complexity of closed-door political negotiations.

These limitations point to several important avenues for future research. Longitudinal studies are needed to track the implementation of the Green Deal and REPowerEU, assessing their long-term impact on the EU's energy mix and dependencies. Further research should focus on the EU's nascent CRM strategy, evaluating its effectiveness in a competitive global market (European Commission, 2023). Finally, detailed political science research is required to understand the precise mechanisms through which populist parties influence specific energy and climate policy files at both the national and EU levels, and to assess the long-term threat they pose to the European Green Deal (Bova, 2011; Hossain & Hallock, 2022).

8. CONCLUSION

The period following Russia's 2022 invasion of Ukraine has been a crucible for the European Union, forcing a fundamental re-evaluation of the nexus between energy security and political stability. What was once a technocratic policy domain has been thrust into the heart of the EU's geopolitical identity, economic strategy, and democratic resilience. The crisis has demonstrated that energy insecurity is not merely an economic vulnerability; it is a potent vector for political instability, capable of generating internal fractures, fueling social unrest, and empowering political movements hostile to the European project itself (Hossain & Hallock, 2022; Bova, 2011).

This report has argued that the EU's political stability is contingent on its ability to manage a formidable policy trilemma between short-term energy security, long-term climate action, and socio-political cohesion. The 2022 energy crisis dangerously exacerbated the tensions between these three imperatives. The EU's response, spearheaded by the REPowerEU plan, was remarkably successful in its immediate goal of decoupling from Russian fossil fuels (European Commission, 2022; Beck et al., 2025). Through a combination of demand reduction, supply diversification via LNG, and an acceleration of renewable deployment, the Union averted a catastrophic energy shortage and demonstrated significant institutional resilience.

However, this success was achieved at a considerable cost. The prioritization of short-term security has led to potential long-term challenges, including the risk of carbon lock-in from new gas infrastructure and the creation of new dependencies on critical raw materials for the green transition (Blondeel et al., 2021; Kowalski & Legendre, 2023). More critically, the crisis has exposed and deepened political fault lines within the Union. Divergent national responses, driven by disparate historical legacies and economic capacities, have strained the single market and the principle of solidarity (Checherita-Westphal & Dorrucci, 2023; Bown, 2024). The resulting energy price inflation created a severe cost-of-living crisis, which in turn fueled a wave of public protests and provided a powerful narrative for populist parties (Hossain & Hallock, 2022). This has created a perilous feedback loop, where the consequences of fossil fuel dependency empower political forces that seek to dismantle the EU's primary long-term solution: the European Green Deal (European Commission, 2023).

The findings of this report underscore a critical reality for the contemporary European Union: energy policy is no longer separable from high politics. The security of the Union is no longer solely a matter of military defense or border control; it is fundamentally intertwined with the resilience of its energy systems, the stability of its supply chains, and the affordability of energy for its citizens and industries. The ability to manage the energy transition is not just an environmental necessity but a geopolitical and democratic imperative (Vakulchuk et al., 2020; IEA, 2025). Successfully navigating this transition—ensuring it is secure, affordable, and just—is synonymous with ensuring the long-term political stability and strategic viability of the European project. Failure to do so risks not only missing climate targets but also eroding social cohesion and undermining the foundations of the Union itself.

As the EU continues to navigate this new and contested landscape, several areas demand further scholarly inquiry. The long-term geopolitical dynamics of a world defined by competition over clean energy supply chains, rather than fossil fuels, require deep analysis (Kowalski & Legendre, 2023). The effectiveness of the EU's industrial policy and CRM strategy in building genuine strategic autonomy will be a critical field of study (European Commission, 2023). Finally, and perhaps most urgently, ongoing research must monitor the evolving political landscape within the EU, analyzing how the growing influence of populist and nationalist parties in Member States and in the European Parliament will shape the implementation and future ambition of the European Green Deal (Hossain & Hallock, 2022; Bova, 2011). The outcomes of these political contests will ultimately determine whether the EU can successfully resolve its energy trilemma and secure a stable, prosperous, and sustainable future.

REFERENCES

Ake, C. (1975). A definition of political stability. *Comparative Politics, 7*(2), 271–283.

Alasuutari, P., & Qadir, A. (2014). Epistemic governance: An approach to the politics of policy-making. *European Journal of Cultural and Political Sociology, 1*(1), 69–87.

Alasuutari, P., & Qadir, A. (2019). The synchronisation of national policies: A new research agenda. *Journal of European Public Policy, 26*(9), 1338–1355.

Babina, T., et al. (2023). *The global reallocation of energy flows* (Working Paper).

Bealey, F. (1999). *The Blackwell dictionary of political science: A user's guide to its terms*. Blackwell Publishers.

Beck, M., et al. (2025). The German energy transition after the Russia-Ukraine war – challenges and opportunities. *Carbon Neutral Systems, 1*(4).

Bialek, S., et al. (2023). *National policies to shield consumers from rising energy prices*. Bruegel.

Blondeel, M., et al. (2021). The geopolitics of the energy transition. *Energy Strategy Reviews, 38*, 100742.

Böhringer, C., & Keller, A. (2011). Energy security: An indicator analysis. *Energy Policy, 39*(12), 7878–7886.

Bova, R. (2011). *How the world works: A brief survey of international relations*. Pearson.

Bown, C. P. (2024). *Economic security: A primer*. Peterson Institute for International Economics.

Carfora, A., et al. (2022). Energy security in Europe: A quantitative analysis. *Energy Economics, 113*, 106225.

Checherita-Westphal, C., & Dorrucci, E. (2023). The fiscal response to the energy crisis in the euro area. *ECB Economic Bulletin*.

Cherp, A., & Jewell, J. (2014). The concept of energy security: Beyond the four As. *Energy Policy, 75*, 415–421.

European Commission. (2019). *The European Green Deal* (COM(2019) 640 final).

European Commission. (2022). *REPowerEU plan* (COM(2022) 230 final).

European Commission. (2023). *Joint communication on a European economic security strategy* (JOIN(2023) 20 final).

Eurostat. (2024). *Energy statistics – an overview*. Eurostat Statistics Explained.

Eurostat. (2025). *EU imports of energy products – latest developments*. Eurostat Statistics Explained.

Ferriani, F., & Gazzani, A. (2023). *The energy crisis and the EU single market*. European Parliament Study.

Goldthau, A. (2008). A public policy perspective on energy security. *International Journal of Public Policy, 3*(1/2), 3–21.

Hafner, M., & Tagliapietra, S. (Eds.). (2020). *The geopolitics of the global energy transition*. Springer.

Hossain, N., & Hallock, J. (2022). *Food, energy and cost of living protests in 2022*. Friedrich-Ebert-Stiftung.

Huntington, S. P. (1968). *Political order in changing societies*. Yale University Press.

IEA. (2023). *What is energy security?*. International Energy Agency.

IEA. (2025). *World energy investment 2025*. International Energy Agency.

IRENA. (2025). *Regional energy transition outlook: European Union*. International Renewable Energy Agency.

Kowalski, P., & Legendre, C. (2023). *Critical minerals and the clean energy transition*. OECD Trade Policy Papers.

Leruth, L., et al. (2022). *How the war in Ukraine is revealing a scramble for minerals*. IMF Working Paper.

Meunier, S., & Nicolaidis, K. (2019). The geopoliticization of European trade and investment policy. *Journal of European Public Policy, 26*(12), 1–20.

Siddi, M. (2017). EU–Russia energy relations: From a liberal to a realist paradigm. *Geopolitics, 22*(4), 832–851.

Vakulchuk, R., Overland, I., & Scholten, D. (2020). Renewable energy and geopolitics: A review. *Renewable and Sustainable Energy Reviews, 122*, 109547.

Yergin, D. (2006). Ensuring energy security. *Foreign Affairs, 85*(2), 69–82.

Lishchynsky, M. (2025). The insider threat: A socio-technical analysis of preventing data breaches and espionage within governmental agencies. Politics & Security, 12(2), 88–103. Doi: 10.54658/ps.28153324.2025.12.2.pp.88-103

THE INSIDER THREAT: A SOCIO-TECHNICAL ANALYSIS OF PREVENTING DATA BREACHES AND ESPIONAGE WITHIN GOVERNMENTAL AGENCIES

Mykhailo Lishchynsky
State University of Information and Communication Technologies
Kyiv, Ukraine
https://orcid.org/0009-0009-0103-9904

Abstract *This article presents a socio-technical analysis of the insider threat phenomenon within governmental and public sector institutions. It argues that effective mitigation requires a dynamic, integrated strategy that moves beyond siloed technical controls to holistically address the interplay between individual psychology, organizational culture, technical architecture, and policy enforcement. The analysis defines the governmental insider threat, distinguishing between malicious, unintentional, and compromised insiders, and demonstrates how this typology maps to distinct root causes within the socio-technical system. Through a detailed examination of the Edward Snowden and Chelsea Manning cases, the article deconstructs the convergence of psychological, cultural, and technical vulnerabilities that precipitate catastrophic breaches. It systematically analyzes contributory factors at the individual level, using the Critical Pathway to Insider Risk (CPIR) model; the organizational level, focusing on culture, leadership, and trust; and the technical level, highlighting architectural weaknesses. The article then evaluates a multi-layered defense-in-depth framework integrating human-centric strategies (e.g., positive deterrence, robust training), technical countermeasures (e.g., Zero Trust Architecture, User and Entity Behavior Analytics), and comprehensive policy frameworks (e.g., Executive Order 13587, NITTF Maturity Framework). The inherent tension between security surveillance and employee privacy is explored, reframing privacy protection as a positive driver of organizational trust and security. The article culminates in a novel, coordinated intervention model and provides actionable policy recommendations for governmental agencies to build a more resilient and secure posture against the threat from within..*

Keywords: Insider Threat, Socio-Technical Systems, Government Security, Data Breaches, Espionage.

1. INTRODUCTION

Governmental agencies are built upon a fundamental paradox: the very trust required for their operation creates their most profound vulnerability. To function, these institutions must grant employees, contractors, and partners authorized access to sensitive facilities, systems, and, most critically, classified national security information (Greitzer et al., 2021). This act of entrustment, however, inherently creates the potential for an insider threat—a trusted individual who uses their legitimate access to cause harm, whether intentionally or unintentionally (Greitzer et al., 2021). This threat is not a modern anomaly but an enduring feature of human history, with a common narrative stretching from Benedict Arnold to the catastrophic unauthorized disclosures of the digital age (Greitzer et al., 2021). The core of the problem is fundamentally human; while technology enables new vectors for harm, the threat actor is a person, making the insider threat a "human problem" that demands a human-centric solution (Greitzer et al., 2021). Consequently, it must be understood as a complex socio-technical phenomenon, where risk emerges from the dynamic interplay of individuals, organizational structures, and technological systems (Hutchins et al., 2016).

To deconstruct this complexity, this article adopts a Socio-Technical Systems (STS) framework as its primary analytical lens. STS theory posits that organizational performance and security are not determined by technical or social elements in isolation, but by their joint optimization (Pasmore et al., 2018). A purely technocentric approach to security, focused on firewalls and perimeter defenses, is demonstrably insufficient for countering the insider threat (Moore et al., 2015). Insiders, by definition, already possess the "keys to the kingdom" and can bypass external defenses (Silowash et al., 2012). Research consistently shows that human factors—such as behavioral choices, cultural norms, and cognitive errors—are paramount in the majority of security failures, whether in prevention, detection, or mitigation (Greitzer & Frincke, 2010). An STS approach, therefore, necessitates a holistic analysis that integrates insights from organizational psychology (to understand individual motivations and behaviors), public administration (to examine culture, leadership, and policy), and cybersecurity (to assess technical controls and architecture) (Nurse et al., 2014). An effective insider threat program cannot be merely "a security program"; it must be a "sustained employee outreach and awareness effort" that fosters a shared responsibility for protection (Greitzer et al., 2021).

The urgency of adopting a socio-technical perspective is amplified by an evolving threat landscape. The post-pandemic shift toward remote and hybrid work models has expanded the attack surface, fostering reliance on less-secure technologies and increasing employee isolation and stress—factors that can heighten vulnerability to exploitation (Greitzer et al., 2021). Simultaneously, foreign adversaries are engaged in an unprecedented effort to collect data on and exploit vulnerable individuals within critical infrastructure and government workforces, turning them into witting or unwitting assets (Greitzer et al., 2021). The increasing frequency and staggering financial impact of insider incidents, which can cost millions per event, underscore the inadequacy of legacy, perimeter-based security models and the critical need for more advanced, integrated defenses (Ponemon Institute, 2022).

A security strategy focused exclusively on malicious actors, who represent only one facet of the problem, will inevitably neglect the systemic factors that cultivate the far more common unintentional and negligent threats. Official definitions from the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of the Director of National Intelligence (ODNI) explicitly include "unintentional" and "unwitting" harm, recognizing that negligence and accidents are significant contributors to overall risk (Greitzer et al., 2021). Research confirms that a majority of insider incidents stem from non-malicious actions and that many malicious insiders begin as loyal employees who are pushed down a path to betrayal by a combination of personal stressors and organizational failures (Cappelli, Moore, & Trzeciak, 2012). A security program that narrowly frames the problem as one of "finding and punishing bad guys" (Shaw, 2006) will fail to address the cultural, training, and system design flaws that enable the full spectrum of insider risk (Carroll, 2021).

Effective insider threat mitigation in the public sector requires a dynamic, integrated strategy that moves beyond siloed controls to holistically address the interplay between individual psychology, organizational culture, technical architecture, and policy enforcement. This article will deconstruct these socio-technical layers, analyze their interactions through historical cases and contemporary models, and synthesize a coordinated intervention framework to enhance agency resilience against the threat from within. The analysis begins by formally conceptualizing the governmental insider threat and establishing a typology based on intent. It then dissects high-profile breaches to reveal the anatomy of socio-technical failures. Following this, the report provides a multi-level analysis of contributory factors—individual, organizational, and technical. It then details an integrated prevention framework, combining human-centric, technical, and policy-based countermeasures. The enduring dilemma of balancing surveillance and privacy is then examined before the article concludes with a proposed best-practice model and actionable policy recommendations for governmental agencies.

2. CONCEPTUALIZING THE GOVERNMENTAL INSIDER THREAT

*Defining the Insider: From Trusted Colleague to Threat Vector***.** In the context of governmental agencies, an "insider" is formally defined as any person who has or has had authorized access to an organization's resources, including its personnel, facilities, information, equipment, networks, and systems (Greitzer et al., 2021). This definition is intentionally broad, encompassing not only direct government employees but also contractors, vendors, temporary staff, and other trusted business partners who are given access to perform their duties (US-CERT, 2012). The defining characteristic of the insider is their position of trust and the legitimate access it confers. The "insider threat" is the potential for that individual to use their authorized access—wittingly or unwittingly—to cause harm (Greitzer et al., 2021). In the public sector, this threat is particularly acute because the harm can extend beyond organizational damage to compromise national security, public safety, and the integrity of government functions (Greitzer et al., 2021). The threat can manifest in numerous ways, including espionage, terrorism, sabotage, workplace violence, corruption, and the unauthorized disclosure of classified or sensitive information (Greitzer et al., 2021).

A Typology of Insiders: Differentiating Intent. A nuanced understanding of insider threats requires differentiating them based on the individual's intent, as the root causes and appropriate mitigation strategies vary significantly for each type. A comprehensive typology is therefore not merely descriptive but serves as a diagnostic tool for an organization's security posture. A high prevalence of accidental incidents, for example, points toward failures in training and system usability, whereas a pattern of malicious acts suggests deeper problems with organizational culture and employee well-being.

The malicious insider is an individual who intentionally uses their authorized access to harm the organization or misappropriate its assets (Carroll, 2021). Their motivations are diverse and can include financial gain (e.g., selling intellectual property), revenge for a perceived wrong (such as being passed over for a promotion), ideological alignment with an external cause, or espionage on behalf of a foreign entity (Carroll, 2021). Malicious insiders can be further categorized:

- *The Lone Wolf*: This individual acts alone, driven by personal grievances or ideology. They leverage their own knowledge of the organization's systems and security weaknesses to execute their attack and avoid detection (Carroll, 2021).
- *The Collaborator*: This insider works in collusion with an external party, such as a competitor or a criminal organization. They may be motivated by payment or coercion, providing the external actor with credentials, insider knowledge, or direct access to bypass security defenses (Carroll, 2021).

The Unintentional Insider. The *unintentional insider*, often representing the largest portion of insider-related incidents, is an individual who causes harm without malicious intent (Carroll, 2021). Their actions stem from carelessness, mistakes, or a lack of security awareness. This category is critical because it highlights vulnerabilities in processes, training, and culture rather than individual malevolence.

o *The Negligent Insider*: This person is generally aware of security policies but chooses to ignore or circumvent them for reasons of convenience or perceived efficiency. Examples include sharing passwords with colleagues, using unauthorized personal devices for work, or failing to install critical security patches (Greitzer et al., 2021). This behavior often points to a weak security culture or policies that are perceived as overly burdensome.

o *The Accidental Insider*: This individual causes a security incident through a genuine mistake. Common examples include sending a sensitive email to the wrong recipient, inadvertently clicking on a phishing link that installs malware, or misconfiguring a cloud storage setting, thereby exposing data (Greitzer et al., 2021). These incidents often reveal gaps in security awareness training and a need for more user-friendly, mistake-proof systems.

The Compromised Insider. The *compromised insider* is a legitimate user whose credentials or system access have been stolen by an external attacker (Carroll, 2021). The employee is an unwitting pawn, and their account is used to masquerade as a trusted entity within the network. This threat type blurs the line between external and internal attacks and underscores the critical importance of robust identity and access management controls. The attacker, operating with the insider's privileges, can access data, install malware, or move laterally through the network, often evading detection for extended periods (Sarkar et al., 2020).

Beyond a Binary: "Insiderness" as a Spectrum of Access and Trust. A sophisticated analysis must move beyond a simple binary distinction between "insider" and "outsider." Instead, *insiderness* should be conceptualized as a non-binary spectrum, where an individual's degree of insiderness is a function of their specific access privileges relative to a particular asset or resource (Bishop, 2005). For example, a senior systems administrator with root-level access to network servers is "more of an insider" with respect to that infrastructure than a policy analyst. However, that same policy analyst, who has access to draft national security directives, is "more of an insider" with respect to that sensitive information. This concept extends to physical access as well; a janitor with keys to a secure facility is an insider with respect to that physical space (Bishop, 2005). This granular understanding is foundational to implementing the Principle of Least Privilege (PoLP), where access controls are tailored not just to a person's role, but to the specific data and resources they absolutely require to perform their duties. It shifts the security focus from a broad "trusted vs. untrusted" model to a more precise, asset-centric model of verifying access rights for every interaction.

3. ANATOMY OF A BREACH: SOCIO-TECHNICAL FAILURES IN HIGH-PROFILE CASES

An examination of seminal insider threat cases reveals the catastrophic potential of socio-technical failures. The breaches perpetrated by Edward Snowden and Chelsea Manning were not the result of a single vulnerability but rather a convergence of individual psychological pressures, permissive organizational cultures, and inadequate technical controls. They serve as foundational case studies demonstrating why a holistic, integrated approach to insider threat mitigation is imperative.

Case Study 1: Edward Snowden – The Social Engineer in a System of Assumed Trust

The 2013 disclosure of approximately 1.7 million classified documents by Edward Snowden, a former National Security Agency (NSA) contractor, exposed global surveillance programs and triggered a worldwide debate on security and privacy (Gelles, 2013). An analysis of the breach through a socio-technical lens reveals a systemic failure built on a flawed model of trust.

- *Socio-Psychological Factors*: Snowden's motivation appears to have been primarily ideological, driven by a belief that the surveillance programs he was exposed to were unconstitutional and that the public had a right to know (Gelles, 2013). This places him in the complex category of a prosocially motivated insider, acting to benefit what he perceived as a greater good ("society") rather than for personal gain or revenge (Gelles, 2013). His case highlights the critical role of whistleblower protections. At the time, legal protections for intelligence community contractors like Snowden were tenuous and lacked clear, enforceable legal rights, potentially leaving disclosure to the media as the only perceived viable channel for raising concerns (Fitzpatrick, 2021). This lack of a trusted internal reporting mechanism is a significant socio-policy failure that can push ideologically motivated insiders toward external disclosure.
- *Organizational & Cultural Vulnerabilities*: The most glaring vulnerability was the NSA's organizational culture. Snowden masterfully exploited a culture of collegial helpfulness to circumvent access controls. He used social engineering tactics, telling an estimated 20 to 25 coworkers that he needed their login credentials to perform his duties as a systems administrator, and they complied (Melley, 2014). This indicates a profound failure in security awareness and a culture where the social norm of helping a coworker overrode the cardinal security rule against sharing passwords. The incident suggests that security awareness training was "sorely lacking," as employees in one of the world's most secure environments fell for a basic social engineering trick (Melley, 2014).
- *Technical & Policy Vulnerabilities*: The Snowden breach was a direct result of "totally inadequate" policies and procedures (Melley, 2014). The primary technical failure was a breakdown in identity and access management. The system allowed for, and the culture tolerated, the sharing of login credentials. As a privileged user (systems administrator), Snowden already had significant access, but he was able to aggregate further privileges by using his colleagues' Public Key Infrastructure (PKI) certificates to access classified information on the NSANET (Gelles, 2013). This represents a complete violation of the Principle of Least Privilege. Furthermore, the systems in place lacked sufficient auditing and data exfiltration monitoring to detect and flag the anomalous activity of one user accessing data with multiple credentials and downloading vast quantities of information.

Case Study 2: Chelsea Manning – A Cry for Help in the Digital Panopticon

In 2010, Chelsea Manning, then a U.S. Army intelligence analyst stationed in Iraq, disclosed nearly 750,000 classified and sensitive military and diplomatic documents to the whistleblowing platform WikiLeaks (Greenwald, 2014). Her case illustrates how severe personal distress, when combined with an unsupportive organizational environment and permissive technical access, can lead to a devastating security breach.

- *Socio-Psychological Factors*: Manning's actions were precipitated by a confluence of intense personal and professional stressors. She was grappling with her gender identity in a military environment governed by the "Don't Ask, Don't Tell" policy, which was hostile to LGBTQ+ service members and particularly to transgender individuals (Greenwald, 2014). This personal struggle was compounded by a profound moral conflict over the content of the information she was tasked with analyzing, which included videos of civilian casualties in Iraq and Afghanistan (Sontag, 2014). Her personal history, which included a difficult upbringing and being bullied, likely contributed to her feelings of alienation and a desire to act (Greenwald, 2014). Her disclosures can be interpreted as a dissident act of protection—"if you cannot protect me from my secrets, then I will not protect you from yours"—stemming from a feeling of being an "unprotectable" subject within the military's logic of security (Sontag, 2014).
- *Organizational & Cultural Vulnerabilities*: The organizational environment was a critical catalyst. Manning was described as "extremely isolated from her unit," indicating a significant failure of leadership, NCO supervision, and peer support systems (Sontag, 2014). Her defense team argued that supervisors failed to act on clear behavioral indicators of her mental and emotional distress, suggesting a breakdown in the military's duty of care and a failure to recognize that personnel well-being is a component of security (Sontag, 2014). The institutional culture, which at the time did not recognize or support transgender individuals, created an environment where her personal struggles were intensified rather than mitigated (Sontag, 2014).
- *Technical & Policy Vulnerabilities*: As a cleared intelligence analyst, Manning was granted broad access to classified databases, including the Secret Internet Protocol Router Network (SIPRNet) (Greenwald, 2014). The critical technical failure was the absence of effective data loss prevention (DLP) and endpoint monitoring controls. She was able to download hundreds of thousands of documents onto recordable CDs, which she reportedly labeled with titles like "Lady Gaga," without triggering any automated security alerts (Greenwald, 2014). This demonstrates a gaping vulnerability in monitoring data exfiltration to removable media. The system's security posture was predicated on trusting the cleared user, failing to scrutinize the user's behavior on the network. Access was granted based on role, not on a granular, need-to-know basis, and the system lacked the capability to detect and flag such a large and anomalous data transfer.

The Snowden and Manning cases, while different in motivation and method, both expose a fundamental flaw in legacy security models: the "trust-but-don't-verify" paradigm. Both individuals were granted enormous trust based on a static attribute—their security clearance. This initial grant of trust, a social and administrative construct, led to a dangerous relaxation of continuous technical verification. Snowden exploited the social layer of this trust, while Manning exploited the technical layer. The systems implicitly assumed that a trusted person would always behave in a trustworthy manner, a catastrophic miscalculation. These two breaches serve as the foundational justification for the shift toward a Zero Trust Architecture, which is built on the opposite principle: "Never Trust, Always Verify" (Rosenbach & Peritz, 2009).

Table 1: Comparative Analysis of Insider Threat Case Studies (Snowden & Manning)

Socio-Technical Dimension	**Case 1: Edward Snowden**	**Case 2: Chelsea Manning**
Insider Type & Motivation	Malicious (Ideological/Prosocial). Motivated by a belief that government surveillance was unconstitutional and a desire to inform the public (Greenwald, 2014).	Malicious (Moral/Psychological). Motivated by profound moral conflict over war conduct and severe personal distress related to gender identity and isolation (Sontag, 2014).
Psychological State	Principled dissent and a calculated decision to leak. Acted from a position of intellectual and ethical opposition to policy (Rosenbach & Peritz, 2009).	Extreme emotional distress, isolation, and moral injury. Actions were intertwined with a personal crisis and a cry for help (Sontag, 2014).

Socio-Technical Dimension	Case 1: Edward Snowden	Case 2: Chelsea Manning
Organizational Culture	Exploited a culture of collegial helpfulness that overrode security protocols. Security awareness was secondary to job expediency (Savage, 2016).	An unsupportive and isolating unit culture that exacerbated personal distress. A command climate that was hostile to gender non-conformity (Sontag, 2014).
Leadership & Peer Support	Colleagues were willing accomplices, albeit through social engineering. Indicates a lack of critical security thinking among peers (Savage, 2016).	Catastrophic failure of leadership and peer support. Supervisors allegedly ignored clear behavioral indicators of severe distress (Sontag, 2014).
Technical Vulnerability (Access Control)	Exploited weak identity controls by socially engineering colleagues for their credentials. Abused his privileged system administrator role to aggregate access (Greenwald, 2014).	Granted overly broad access to classified databases based on her role as an analyst. Lack of granular, need-to-know access restrictions on the network (Greenwald, 2014).
Technical Vulnerability (Data Exfiltration)	Inadequate auditing and monitoring to detect large-scale data harvesting from multiple user accounts. Focus was on perimeter, not internal activity (Greenwald, 2014).	Complete failure of endpoint security and Data Loss Prevention (DLP). Allowed mass download of data to removable media (CDs) without detection or prevention (Greenwald, 2014).
Policy Failure	Inadequate whistleblower protections for intelligence contractors, leaving external disclosure as a perceived viable option. Ineffective enforcement of policies against password sharing (Rosenbach & Peritz, 2009).	Lack of policies to support transgender service members. Failure to integrate personnel well-being policies with security protocols, treating them as separate issues (Sontag, 2014).
Primary Lesson	Static trust in credentials is a fatal flaw. Social engineering can defeat technical controls if the human element is untrained and the culture is permissive.	Personal well-being is a critical component of national security. Ignoring psychological distress in cleared personnel creates unacceptable risk.

4. A MULTI-LEVEL ANALYSIS OF CONTRIBUTORY FACTORS

To construct an effective defense, it is necessary to systematically deconstruct the factors that contribute to insider risk. A socio-technical analysis organizes these factors into three interconnected levels: the individual, the organizational, and the technical. These levels do not operate in isolation but form a dynamic feedback loop where vulnerabilities at one level can create or amplify risks at another.

4.1 THE INDIVIDUAL LEVEL: PSYCHOLOGICAL AND BEHAVIORAL DIMENSIONS

At the core of any insider incident is an individual. Understanding their psychological landscape and behavioral trajectory is crucial for detection and mitigation.

The Critical Pathway to Insider Risk (CPIR)

The Critical Pathway to Insider Risk (CPIR) is a widely accepted model in the insider threat community that provides a framework for understanding how a trusted individual transitions toward committing a harmful act (Shaw & Sellers, 2015)[1]. Developed by Dr. Eric Shaw, the model is not a rigid, linear progression but a flexible framework that describes an accumulation of risk over time (Shaw & Sellers, 2015; US CERT, 2012)[2]. The key components are:

- **Personal Predispositions:** These are the foundational vulnerabilities an individual brings to the organization. They include enduring personality traits (e.g., narcissism, low agreeableness, ethical flexibility), psychological conditions (e.g., substance abuse disorders), a history of rule violations, poor social skills, or significant personal vulnerabilities like financial instability (Shaw & Sellers, 2015). These factors do not destine an individual to become a threat, but they lower the threshold for them to react negatively to stressors.

- **Stressors:** These are the triggers—personal or professional—that can activate underlying predispositions and accelerate an individual's movement down the critical pathway. Professional stressors might include a poor performance review, being passed over for promotion, or interpersonal conflict with a supervisor. Personal stressors can include financial hardship, divorce, or the death of a family member (Shaw & Sellers, 2015).
- **Concerning Behaviors:** As an individual struggles to cope with the interaction of predispositions and stressors, they often exhibit observable behaviors that signal escalating risk. These can range from counterproductive work behaviors like absenteeism, tardiness, and poor performance to more alarming signs like expressions of disgruntlement, anger management issues, testing security boundaries, or unexplained affluence (Shaw & Sellers, 2015).
- **Problematic Organizational Response:** This is a critical, and often final, catalyst. How the organization responds to an employee's concerning behavior can either de-escalate the situation or push them further down the path. A heavy-handed, punitive, or dismissive response can intensify feelings of injustice and disgruntlement, while a supportive, fair, and proactive intervention can provide an "off-ramp" from the pathway (Vrieze, 2022)

Observable Behavioral Indicators

The CPIR model is operationalized through the observation of specific behavioral indicators. These fall into two broad categories: technical and psychosocial. Technical indicators are often captured by monitoring systems and include activities like accessing data at unusual hours, attempting to access unauthorized files, escalating privileges, using unapproved software, or downloading abnormally large volumes of data (Cappelli et al., 2012). Psychosocial indicators are observed through human interaction and can include increased disgruntlement and dissatisfaction, confrontational behavior, social withdrawal, expressions of divided loyalty, or signs of financial distress or substance abuse (Shaw & Sellers, 2015). A significant challenge is that many of these indicators are ambiguous on their own; an employee working late could be dedicated or preparing to exfiltrate data. Therefore, effective analysis requires gathering and integrating multiple indicators to see a converging pattern of risk (Greitzer et al., 2012).

Critiques and Limitations of Behavioral Models

While behavioral models like the CPIR are invaluable for framing the problem, they have limitations. The primary statistical challenge is predicting a low base-rate event; espionage and major sabotage are rare, making it difficult to build a predictive model with high accuracy and low false positives (Shaw & Sellers, 2015). The CPIR is a powerful heuristic for analysis and intervention, but it is not an infallible predictive tool. Critics and developers of the model acknowledge open questions regarding its full validation against agreed-upon criteria and the difficulty of precisely weighing the relative importance of different stressors and predispositions, which may interact in non-linear ways (Greitzer et al., 2012). The pathway is not always a simple, sequential progression, and organizational factors can be impactful at any point (Cappelli et al., 2012).

4.2 THE ORGANIZATIONAL LEVEL: CULTURE, LEADERSHIP, AND TRUST

The organization is not a passive backdrop but an active participant in the creation and mitigation of insider risk. Its culture, leadership, and approach to trust can either build resilience or cultivate the conditions for a breach.

Organizational Culture as a Security Control

Organizational culture—the shared beliefs, values, and norms that shape employee behavior—is a critical, albeit often overlooked, security control (Greitzer & Frincke, 2010). A toxic work environment characterized by perceptions of injustice, lack of support, or excessive pressure can directly cause or intensify the stressors that drive insider threats (Shaw & Sellers, 2015; Greitzer et al., 2012). Research shows a substantial relationship between employees' perception of injustice and deviant behavior like theft and sabotage (Willison & Warkentin, 2013). Conversely, a positive and "culturally competent" organization that values fairness, diversity, inclusion, and employee well-being fosters a sense of loyalty and psychological safety (Greitzer & Frincke, 2010). In such a culture, employees are more likely to internalize the organization's goals, voluntarily comply with security policies, and feel empowered to report concerns without fear of retaliation (Cappelli et al., 2012).

The Role of Ethical Leadership and Communication

Leadership is the primary architect of organizational culture (Greitzer & Frincke, 2010). In the context of public administration, ethical leadership grounded in principles of honesty, justice, respect, integrity, responsibility, and transparency is foundational to building public trust and ensuring effective governance (Brown & Treviño, 2006). This extends directly to insider threat mitigation. Leaders who model ethical behavior and communicate the importance of security and integrity set a powerful tone from the top (Shaw & Sellers, 2015). Communication must be clear, consistent, and transparent, especially regarding security policies and monitoring practices (Willison & Warkentin, 2013). Explaining the "why" behind security measures helps build buy-in and prevents the insider threat program from being perceived as a punitive, distrustful "Big Brother" initiative, thereby fostering the trust necessary for its success (Shaw & Sellers, 2015).

The Trust-Control Paradox

Government agencies face an inherent tension between the need to trust employees and the need to implement controls—the trust-control paradox. While trust is essential for morale and operational effectiveness, unchecked trust is a vulnerability. However, implementing overly intrusive surveillance and controls can erode morale, damage the psychological contract, and foster a culture of suspicion (Cappelli et al., 2012). This can be counterproductive, creating the very disgruntlement and resentment that the program aims to prevent. The key is to strike a defensible balance by achieving “proportionality” in surveillance, focusing monitoring on high-risk activities and critical assets rather than blanket observation, and being transparent about the process (Cappelli et al., 2012).

4.3 THE TECHNICAL LEVEL: SYSTEMIC AND ARCHITECTURAL VULNERABILITIES

Technical systems and their architecture can either provide robust defenses or create fertile ground for insider threats to flourish.

- *The Principle of Least Privilege (PoLP)*

A foundational source of technical vulnerability is the systemic failure to enforce the Principle of Least Privilege. Insiders, both malicious and unintentional, often have access privileges far exceeding what is necessary for their job functions (Cappelli et al., 2012). This “privilege creep” occurs through common but dangerous practices like permission inheritance, where a new employee’s access rights are simply cloned from a colleague’s profile, or the failure to revoke temporary, elevated privileges after a specific task is completed (Cappelli et al., 2012). Every unnecessary permission is an attack vector waiting to be exploited.

- *Insufficient Access Control and Auditing*

Weaknesses in Identity and Access Management (IAM) are a primary technical enabler of insider threats. A lack of strictly enforced multi-factor authentication (MFA) makes it significantly easier for an attacker to use compromised credentials, whether they were stolen from the insider or by the insider from a colleague (Cappelli et al., 2012). Compounding this is the problem of inadequate auditing. Without comprehensive and centralized logging of user activities—such as file access, system commands, and network connections—and the tools to analyze these logs for anomalies, it becomes nearly impossible to detect malicious or high-risk behavior in a timely manner (Brdiczka et al., 2012).

- *Data Exfiltration Pathways*

Finally, technical vulnerabilities manifest as open pathways for data exfiltration. These include unsecured endpoints that allow the connection of unauthorized removable media like USB drives, which was a key failure in the Manning case (Brdiczka et al., 2012). They also include poorly monitored network egress points, where large data transfers can go unnoticed. A significant and growing vulnerability is the use of *shadow IT*—unsanctioned cloud services, messaging apps, or other software that employees use to circumvent official, more restrictive channels, thereby bypassing security controls entirely (Greitzer & Frincke, 2010).

The interaction between these three levels is not linear but cyclical. A technical vulnerability, such as the ability to download data to a USB drive, provides an opportunity. An individual experiencing financial stress may have the motivation to exploit it. However, it is the organizational culture that acts as the critical modulator. A supportive culture may provide the employee with an off-ramp, such as an employee assistance program, constraining the behavior. A toxic culture may amplify the motivation, encouraging the act. If the act is attempted and the organization's response is weak, it provides positive reinforcement, encouraging further, more severe actions and completing a dangerous feedback loop. This demonstrates that technical controls alone are insufficient; the "blast radius" of a technical flaw is ultimately determined by the organizational environment in which it exists.

5. AN INTEGRATED FRAMEWORK FOR PREVENTION AND MITIGATION

An effective defense against the insider threat cannot rely on a single solution but requires a multi-layered, defense-in-depth strategy that integrates human-centric, technical, and policy interventions. This socio-technical framework addresses risk at every stage, from preventing individuals from starting down the critical pathway to mitigating the impact of an incident that has already occurred.

5.1 HUMAN-CENTRIC STRATEGIES: THE FIRST LINE OF DEFENSE

Because the insider threat is a human problem, the most effective strategies begin with the workforce itself. The goal is to build a resilient, security-conscious culture that acts as the first and most crucial line of defense.

- *Effective Security Awareness and Training*

Annual, "check-the-box" security training is insufficient. An effective program requires a continuous vigilance campaign that keeps security top-of-mind. Best practices, as promoted by the Center for Development of Security Excellence (CDSE), involve using a variety of engaging methods, including real-world case studies, interactive games, and frequent, targeted messaging through multiple channels (CDSE, 2021). The primary objective of this training is to move beyond mere compliance and cultivate a proactive security culture. It aims to empower every employee to function as part of a "human sensor" network, capable of recognizing the behavioral and technical indicators of a potential threat and knowing how to report them through trusted, confidential channels (CISA, 2022).

The Formal Insider Threat Program (ITP)

As mandated by federal policy, a formal, centralized Insider Threat Program (ITP) is the organizational cornerstone of this strategy. An effective ITP is not just a security function but a multi-disciplinary hub that brings together expertise from Human Resources, legal counsel, privacy and civil liberties officers, security, counterintelligence, and information technology (Greitzer & Frincke, 2010). Governed by a designated senior official with clear authority and resources, the program's mandate is to gather, integrate, and analyze information from across the organization to detect potential threats (NITTF, 2020). Crucially, the program's philosophy should be geared toward proactive mitigation and intervention. The goal is to identify individuals who are on the critical pathway and provide "off-ramps"—such as counseling, financial assistance, or managerial intervention—to resolve the underlying issues before they escalate into a security incident. The mantra is to "turn people around, not turn them in" (Shaw & Sellers, 2015).

- *Positive Deterrence*

Complementing the formal controls of an ITP is the strategy of positive deterrence. This approach seeks to reduce insider risk not through fear of punishment (negative deterrence) but by aligning the interests of the employee with those of the organization. It is rooted in organizational psychology and focuses on increasing Perceived Organizational Support (POS)—the employee's belief that the organization values their contribution and cares about their well-being. Agencies can foster POS through practices such as ensuring procedural and distributive justice (fairness in processes and outcomes), providing robust employee support and development programs, and training managers to be supportive and respectful (Cohen, 2021). By reducing the disgruntlement, stress, and feelings of injustice that often motivate malicious acts, positive deterrence increases voluntary compliance with security policies and builds a more loyal, engaged, and resilient workforce (Shaw et al., 1998).

- *Whistleblower Protections*

A robust, accessible, and trusted whistleblower protection program is a critical safety valve within a governmental agency. When employees believe they have a legitimate and safe channel to report waste, fraud, abuse, or other misconduct, it can prevent them from concluding that an unauthorized public disclosure is their only recourse (Shaw & Sellers, 2015). The Snowden case, in part, highlights the potential consequences of inadequate protections for contractors within the intelligence community (Pope, 2019). Strong protections are not antithetical to security; they are a component of an ethical and transparent culture that builds trust and can preempt damaging leaks by providing an alternative, sanctioned path for dissent.

5.2 TECHNICAL COUNTERMEASURES: BUILDING A RESILIENT ARCHITECTURE

Human-centric strategies must be reinforced by a robust technical architecture designed to limit opportunity and detect anomalous behavior. Modern defenses move beyond static, perimeter-based models to adopt dynamic, data-centric approaches.

- *Monitoring and Analytics (UEBA & DLP)*

• User and Entity Behavior Analytics (UEBA): UEBA solutions are a cornerstone of modern insider threat detection. These systems use machine learning and advanced analytics to establish a dynamic baseline of normal behavior for each user and entity (e.g., servers, devices) on the network. They then continuously monitor for deviations from this baseline. For an insider threat, this is critical for detecting actions that are technically authorized but behaviorally anomalous—for example, a network administrator who suddenly begins accessing large numbers of HR files at 3:00 AM (CISA, 2022). UEBA is particularly effective at identifying compromised credentials, as the external attacker's behavior will almost certainly differ from that of the legitimate user (King, 2022).

• Data Loss Prevention (DLP): DLP technologies are designed to prevent the unauthorized exfiltration of sensitive data. They function by first identifying and classifying sensitive data (e.g., classified information, Personally Identifiable Information (PII)) and then enforcing policies to control its movement. A DLP system can monitor data at rest (on servers), in use (on an endpoint), and in motion (across the network) (Pomerleau, 2021). It can automatically block an employee from emailing a classified document to a personal account, copying sensitive files to an unauthorized USB drive, or uploading them to a non-sanctioned cloud service (Watson, 2020). While implementation can be complex and face delays in large government environments, when operational, DLP provides a critical technical backstop against data breaches (DoD Cyber Exchange, 2022).

- *The Zero Trust Mandate*

The most significant strategic shift in government cybersecurity is the mandate to adopt a Zero Trust Architecture (ZTA), as directed by Executive Order 14028 (Office of the President, 2021). ZTA represents a fundamental paradigm shift away from the flawed "trust but verify" model.

• Core Principles: The foundational tenets of ZTA are "Never trust, always verify," the Principle of Least Privilege, and micro-segmentation (NIST, 2020). A ZTA assumes the network is already compromised ("assume breach") and therefore scrutinizes every single access request. Trust is never granted implicitly based on network location (i.e., being "inside" the firewall) or a one-time login (Walsh, 2021).

• Application to Insider Threats: ZTA is a powerful countermeasure to insider threats. By enforcing least privilege access, it ensures an insider can only access the specific data and applications they need to do their job, dramatically reducing the potential damage they can cause. Micro-segmentation prevents an insider (or a compromised account) from moving laterally across the network to access other systems. Most importantly, ZTA replaces the static trust model that failed in the Snowden and Manning cases with a system of continuous, dynamic authentication and authorization. Every request to access a resource is re-evaluated in real-time based on the identity of the user, the health of their device, the location, and other contextual signals (DoD CIO, 2022). The Department of Defense's comprehensive ZTA implementation strategy serves as a key roadmap for other agencies (Office of the President, 2021).

5.3 POLICY AND LEGAL SCAFFOLDING: MANDATES AND FRAMEWORKS

The human and technical strategies operate within a comprehensive policy and legal framework established to govern insider threat programs across the U.S. government.

- *Executive Order 13587 and the National Insider Threat Policy*

Issued in the wake of major leaks, Executive Order 13587 is the foundational directive for federal insider threat programs. It mandates that all executive branch agencies with access to classified information establish programs to deter, detect, and mitigate insider threats (Office of the President, 2011). The accompanying National Insider Threat Policy sets forth minimum standards, including requirements for monitoring user activity on classified networks, providing comprehensive employee awareness training, establishing a multi-disciplinary analysis hub, and ensuring robust protections for privacy, civil rights, and civil liberties (White House, 2012).

- *The NITTF Maturity Framework*

To help agencies move beyond simple compliance, the National Insider Threat Task Force (NITTF) developed the Insider Threat Program Maturity Framework. This framework provides a detailed roadmap for continuous improvement, outlining 19 maturity elements across key areas such as program leadership, personnel, training, access to information, user activity monitoring, and data analytics (NITTF, 2018). It allows agencies to self-assess their capabilities against best practices and identify specific areas for investment and enhancement, fostering a more proactive and effective security posture (NITTF, 2018).

- *Program Evaluation*

A critical policy component is the requirement for effective program evaluation. This presents a significant challenge, as "magic metrics" do not exist (CISA, 2022). Effective evaluation requires moving beyond simple operational metrics (e.g., number of alerts generated, cases closed) to develop programmatic metrics that measure actual risk reduction and alignment with organizational objectives (CISA, 2022). While it is difficult to prove how many incidents were prevented, a mature program can demonstrate its value through indicators of reduced vulnerability, faster detection times, and successful, non-punitive interventions. Meaningful metrics are essential for justifying program resources and maintaining support from senior leadership (CISA, 2022).

The strategies of positive deterrence and Zero Trust, while seemingly operating at opposite ends of the trust spectrum, are not contradictory but deeply synergistic. Positive deterrence aims to build social and psychological trustworthiness in the human actor, reducing their intent to cause harm. Zero Trust eliminates implicit technical trust in the system, continuously verifying the actor's access regardless of their intent. An employee cultivated in a high-trust, supportive environment is less likely to try to circumvent ZTA controls and more likely to understand their necessity. In turn, ZTA provides the hard guardrails that contain the damage from the rare malicious actor or the more common accidental error. A truly mature program integrates both, using culture to reduce the likelihood of an attempt and architecture to reduce the impact of any attempt that occurs.

6. THE ENDURING DILEMMA: BALANCING SURVEILLANCE, PRIVACY, AND TRUST

The implementation of any effective insider threat program inevitably confronts one of the most challenging ethical and legal dilemmas in modern governance: the balance between the state's need for security surveillance and the public employee's right to privacy. Navigating this conflict is not merely a matter of legal compliance but is central to the program's ultimate success or failure.

- *The Legal and Ethical Landscape*

In the United States, public sector employees do not forfeit all privacy rights at the workplace door. The Fourth Amendment provides protection against unreasonable searches and seizures, a principle that the Supreme Court has extended to the workplace in cases like *O'Connor v. Ortega*, which established that employees may have a reasonable expectation of privacy, balanced against the government's legitimate interests in supervision, efficiency, and security (Department of Justice, 2021). This balance is further governed by a complex web of statutes, such as the Privacy Act of 1974, which regulates the government's collection and use of personally identifiable information (U.S. Congress, 1974). From an ethical standpoint, any monitoring must be necessary and proportionate to the risk being mitigated; it cannot be a boundless digital fishing expedition (Wright & Kreissl, 2014).

- *The Psychological Impact of Surveillance*

The implementation of surveillance technologies, if handled poorly, can have a profoundly negative psychological impact on the workforce. Pervasive or opaque monitoring can create a "chilling effect," where employees alter their behavior and censor their communications out of fear of being watched or misinterpreted (Kamal, 2016). This erodes morale and fosters a culture of mistrust, directly undermining the psychological contract between the employee and the organization (Carroll, 2019). This outcome is not only detrimental to productivity and well-being but is actively counterproductive to the goals of the insider threat program. A workforce that feels constantly suspected and distrusted is more likely to become disgruntled, creating the very psychological conditions that can lead to insider threats (Cappelli, Moore, & Trzeciak, 2012).

- *Strategies for Achieving a Defensible Balance*

Striking a sustainable and legally defensible balance requires a deliberate, principled approach that integrates privacy protection into the very design of the insider threat program. This reframes privacy not as an obstacle to security, but as a critical enabler of it. When employees trust that their privacy is being respected, they are more likely to trust the organization and its security mission, leading to greater engagement, higher morale, and an increased willingness to act as partners in security by reporting genuine threats. This creates a virtuous cycle: robust privacy practices build employee trust, which in turn reduces malicious intent and increases voluntary reporting, thereby enhancing overall security.

Key strategies for achieving this balance include:

o Transparency and Communication: Agencies must be unequivocally transparent with their workforce about monitoring activities. This includes establishing clear, accessible policies that detail what information is collected, for what specific security purposes it is used, how it is protected, and who can access it (Cappelli, Moore, & Trzeciak, 2012). This transparency should be reinforced through mandatory training and conspicuous network login banners that inform users of monitoring for lawful government purposes (Executive Office of the President, 2011).

o Proportionality and Data Minimization: The scope of monitoring must be proportional to the risk. The goal is to protect the organization's "crown jewels," not to engage in "Big Brother" surveillance of the entire workforce (Cappelli, Moore, & Trzeciak, 2012). This principle of data minimization dictates that agencies should only collect and retain the specific data necessary to identify high-risk indicators, and for no longer than required (Department of Justice, 2021). Risk-based monitoring, which focuses on high-privilege users or anomalous activities, is preferable to indiscriminate surveillance.

o Oversight and Due Process: A multi-disciplinary governance body, which must include officials from the Office of General Counsel and the agency's privacy and civil liberties offices, is essential for providing independent oversight (Office of the Director of National Intelligence, 2017). This body must review and approve monitoring policies to ensure they are legally and ethically sound. Furthermore, there must be a clear, fair, and documented process for investigating alerts generated by monitoring systems, with avenues for employees to contest findings and correct inaccuracies in their records (Wright & Kreissl, 2014).

o Privacy Impact Assessments (PIAs): Before deploying any new monitoring technology, agencies should be required to conduct a thorough Privacy Impact Assessment (Department of Justice, 2021). A PIA is a formal process used to identify and mitigate potential privacy risks, ensuring that the technology's security benefits are weighed against its impact on individual privacy and that appropriate safeguards are built in from the start.

7. CONCLUSION: A COORDINATED MODEL FOR MINIMIZING INSIDER RISK

The insider threat is an enduring and complex challenge for governmental agencies, rooted in the paradox of trust. This analysis has demonstrated that the threat is not a monolithic problem solvable by a single tool or policy, but a multifaceted socio-technical phenomenon. The catastrophic breaches perpetrated by individuals like Edward Snowden and Chelsea Manning were not simple technical failures or isolated acts of troubled individuals; they were systemic breakdowns resulting from the convergence of psychological vulnerabilities, permissive organizational cultures, and inadequate technical and policy guardrails

(Brackney & Anderson, 2004; Shaw & Sellers, 2015). Effective prevention and mitigation, therefore, demand a departure from siloed, technocentric approaches. A resilient defense must be built on an integrated framework that jointly optimizes human, technical, and policy interventions, recognizing that these elements are inextricably linked in a dynamic system. A failure in one domain, such as a toxic culture, can neutralize the effectiveness of even the most advanced technical controls (Cappelli, Moore, & Trzeciak, 2012).

To translate this socio-technical imperative into an operational strategy, this article proposes a Coordinated Human–Technology–Policy Intervention Model. This model, detailed in Table 2, provides a holistic, defense-in-depth framework for insider risk management. It structures interventions across three critical domains—Human-Centric, Technical Controls, and Policy & Governance—and applies them at each stage of the risk lifecycle: Prevention & Deterrence, Detection & Analysis, and Mitigation & Response. This integrated model moves beyond a simple checklist of best practices to illustrate how different interventions must be coordinated to be effective. For example, preventing insider threats requires not only Zero Trust architecture (technical) but also a culture of psychological safety (human) and clear acceptable use rules (policy) (Department of Defense, 2023; Office of the Director of National Intelligence, 2017; National Insider Threat Task Force, 2020). By mapping interventions in this way, the model provides a practical and comprehensive roadmap for agency leaders and program managers to table2.

Table 2: A Coordinated Human–Technology–Policy Intervention Model for Insider Risk

Stage of Risk Management	A. Human-Centric Interventions	B. Technical Controls	C. Policy & Governance
1. Prevention & Deterrence	**Build a Resilient Workforce:** • Implement continuous, engaging, and behavior-based security awareness training and vigilance campaigns (CDSE, 2020). • Foster a culture of psychological safety, trust, and fairness through ethical leadership and supportive management (DeGraaf et al., 2018). • Actively promote Employee Assistance Programs (EAPs) and other wellness resources to provide "off-ramps" for stressed employees (Shaw & Sellers, 2015). • Implement "positive deterrence" strategies to align employee and organizational interests and reduce disgruntlement (Lind et al., 2001).	**Harden the Architecture:** • Implement a Zero Trust Architecture (ZTA) based on the principles of "never trust, always verify," least privilege, and micro-segmentation (Kindervag, 2010; Executive Office of the President, 2021). • Enforce strong Identity and Access Management (IAM), including mandatory phishing-resistant Multi-Factor Authentication (MFA) for all users (CISA, 2021). • Secure endpoints by controlling the use of removable media and unsanctioned software ("shadow IT") (Greitzer et al., 2012). • Classify all sensitive data and apply encryption at rest and in transit (Ponemon Institute, 2023).	**Establish Clear Guardrails:** • Develop and enforce clear, unambiguous policies for acceptable use, data handling, and remote work (Solove, 2008). • Mandate and resource a formal, multi-disciplinary Insider Threat Program (ITP) with a designated senior official (ODNI, 2017). • Establish and promote a trusted, accessible, and legally robust Whistleblower Protection Program (Devine, 2015). • Conduct thorough pre-employment screening and continuous vetting for all personnel with privileged access (NITTF, 2020).
2. Detection & Analysis	**Empower the Human Sensor Network:** • Train all personnel to recognize and report concerning behavioral and technical indicators via clear, confidential channels (CDSE, 2020). • Utilize the Critical Pathway to Insider Risk (CPIR) model as an analytical framework for the ITP hub to assess cases (Shaw & Sellers, 2015). • Involve behavioral science professionals in the analysis hub to help contextualize behaviors and reduce bias (NITTF, 2020). • Foster supervisor skills in recognizing and addressing concerning conduct early and appropriately (NITTF, 2020).	**Enable Data-Driven Visibility:** • Deploy and integrate User and Entity Behavior Analytics (UEBA) and Data Loss Prevention (DLP) tools (Gartner, 2023). • Use AI/ML to baseline normal user behavior, detect significant deviations, and assign risk scores to prioritize alerts (Ponemon Institute, 2023). • Correlate technical alerts from network, endpoint, and application logs with data from HR systems (e.g., performance reviews) and physical access logs (ODNI, 2017). • Maintain comprehensive, centralized, and attributable audit logs for all critical systems (CDSE, 2020).	**Define Analytical Governance:** • Mandate information sharing across agency silos (HR, Security, IT, Legal) to the central ITP analysis hub (ODNI, 2017). • Conduct Privacy Impact Assessments (PIAs) for all monitoring and analytics tools to ensure compliance and proportionality (Gellman, 2013). • Adhere to the NITTF Maturity Framework to guide the evolution of analytical capabilities (NITTF, 2020). • Establish formal procedures for validating and integrating new data sources into the analytical process (NITTF, 2020).

Stage of Risk Management	A. Human-Centric Interventions	B. Technical Controls	C. Policy & Governance
3. Mitigation & Response	**Prioritize Human-Centered Intervention:** • For non-malicious incidents, focus on corrective action, retraining, and addressing root causes (e.g., process flaws, usability issues) (Greitzer & Frincke, 2010). • For at-risk individuals, deploy supportive interventions (e.g., EAP referral, managerial support) to provide an "off-ramp" from the critical pathway (Shaw & Sellers, 2015). • Ensure all interactions are handled with fairness and respect to avoid exacerbating disgruntlement (avoid "problematic organizational responses") (Brackney & Anderson, 2004). • Maintain open communication with the workforce about the program's positive outcomes and supportive mission (DeGraaf et al., 2018).	**Execute Automated & Manual Response:** • Use Security Orchestration, Automation, and Response (SOAR) to automate initial responses to high-confidence alerts (CISA, 2021). • For active investigations, dynamically adjust access controls, increase monitoring levels, or isolate compromised systems to contain damage (ODNI, 2017). • Conduct thorough digital forensics to determine the full scope of an incident and preserve evidence (NITTF, 2020). • Ensure the ITP itself is audited to prevent misuse of powerful monitoring tools by its own personnel (NITTF, 2020).	**Ensure Legal & Procedural Integrity:** • Operate under a formal, legally vetted Incident Response Plan that defines roles, responsibilities, and escalation paths (NIST, 2018). • Ensure all mitigation and response actions are conducted with oversight from legal counsel and privacy officials to protect individual rights (ODNI, 2017). • Document all cases, actions, and outcomes in a secure case management system to ensure accountability and enable longitudinal analysis (NITTF, 2020). • Use after-action reports from incidents and exercises to drive continuous improvement of policies, procedures, and controls (NIST, 2018).

8. ACTIONABLE POLICY RECOMMENDATIONS FOR GOVERNMENTAL AGENCIES

Based on the preceding analysis and the integrated model, the following policy recommendations are proposed to strengthen insider threat mitigation across the public sector:

1. *Mandate a Socio-Technical Approach in Program Design and Evaluation.* Federal policy, including updates to the National Insider Threat Policy and agency-specific directives, should explicitly require Insider Threat Programs (ITPs) to be designed, implemented, and evaluated based on a socio-technical framework. This entails moving beyond a checklist of minimum technical standards toward demonstrating how human-centric strategies, technical controls, and policy governance are integrated into a cohesive, mutually reinforcing system. Oversight bodies should assess not only technical capabilities but also the maturity and coherence of this integration (Shaw & Sellers, 2015; NITTF, 2020).

2. *Elevate and Invest in Organizational Culture as a Security Metric.* Agencies should be required to treat organizational culture and psychological safety as core security concerns. This includes allocating resources for ethical leadership development, fostering procedural justice, and creating fair and psychologically safe work environments (Lind et al., 2001). Tools like the Federal Employee Viewpoint Survey (FEVS) should be formally integrated into insider threat assessments, and ITPs must collaborate with Human Resources to respond to organizational climate weaknesses (DeGraaf et al., 2018).

3. *Accelerate and Fully Fund the Zero Trust Mandate.* Congress and the Office of Management and Budget (OMB) must prioritize and enforce comprehensive implementation of Zero Trust Architecture (ZTA) across all agencies. ZTA must be recognized as foundational to insider threat prevention, not merely a cybersecurity upgrade. Its deployment should encompass all pillars of the CISA Zero Trust Maturity Model and be integrated into broader agency transformation initiatives (CISA, 2021; Executive Office of the President, 2021).

4. *Professionalize the Insider Threat Workforce.* The National Insider Threat Task Force (NITTF), in partnership with the Office of Personnel Management (OPM), should establish a formal certification and career development track for insider threat professionals. Given the cross-disciplinary nature of insider threat detection and response, training should include cybersecurity, behavioral science, data analytics, organizational psychology, counterintelligence, and privacy law (CDSE, 2020; NITTF, 2020). Standardized curricula should be developed and mandated for all ITP staff.

5. *Strengthen and Actively Promote Whistleblower Protection Channels*. Inspector General offices should, in partnership with ITP leaders, conduct biennial audits of whistleblower protection programs to assess accessibility and effectiveness. Results should be reported to agency leadership and used to inform reforms. Awareness campaigns and training must frame protected reporting channels as legitimate, trustworthy, and central to the organization's mission—not as adversarial mechanisms (Devine, 2015; Greitzer et al., 2012).

6. *Adopt a "Balanced Deterrence" Policy.* The National Insider Threat Policy should mandate agencies to adopt and assess "positive deterrence" strategies in tandem with traditional security controls. Metrics of insider threat program success must include not only threats detected or incidents responded to but also improvements in employee morale, trust, and organizational support. A well-functioning ITP should be as much a proactive support structure as a reactive enforcement mechanism (Shaw & Sellers, 2015; Lind et al., 2001).

REFERENCES

Ablon, L. (2018). *Assessing the insider threat: Insights from past and present*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR4226.html

Allen, J., & Harper, A. (2020). *IT governance and risk management*. CRC Press.

Andress, J. (2019). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (3rd ed.). Syngress.

Bada, A., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint* arXiv:1901.02672.

Center for Development of Security Excellence (CDSE). (2020). *Insider threat training guide*. https://www.cdse.edu

Center for Internet Security (CIS). (2020). *Controls v8*. https://www.cisecurity.org

CISA. (2021). *Zero Trust Maturity Model*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/zero-trust-maturity-model

DeGraaf, G., Huberts, L., & Smulders, R. (2018). Understanding the research–practice gap in integrity and anti-corruption: The case of the Netherlands. *Public Integrity*, 20(6), 552–566.

Devine, T. (2015). *The corporate whistleblower's survival guide: A handbook for committing the truth*. Berrett-Koehler Publishers.

Executive Office of the President. (2021). *Executive Order 14028 on Improving the Nation's Cybersecurity*. Federal Register, 86(93), 26633–26647.

Federal Chief Information Officers Council. (2020). *Identity, Credential, and Access Management (ICAM) policy*. https://www.cio.gov

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. M., & Ferryman, T. A. (2012). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In *2012 45th Hawaii International Conference on System Sciences* (pp. 2392–2401). IEEE.

Lind, E. A., Kanfer, R., & Earley, P. C. (2001). Voice, control, and procedural justice: Instrumental and noninstrumental concerns in fairness judgments. *Journal of Personality and Social Psychology*, 59(5), 952–959.

National Insider Threat Task Force (NITTF). (2020). *Insider threat program maturity framework*. https://www.dni.gov

O'Connor v. Ortega, 480 U.S. 709 (1987).

Office of the Director of National Intelligence (ODNI). (2012). *National Insider Threat Policy and Minimum Standards*. https://www.dni.gov

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (5th ed.). Pearson.

Reeves, M., & Whitaker, K. (2020). *The zero trust security playbook*. O'Reilly Media.

Relyea, H. C. (2008). The Privacy Act of 1974: A brief legislative history. *Government Information Quarterly*, 25(3), 370–376.

Shaw, E., & Sellers, L. (2015). Application of the Critical-Path Method to evaluate insider risks. *Studies in Intelligence*, 59(2), 1–11.

United States Government Accountability Office (GAO). (2018). *Cybersecurity: Agencies need to improve implementation of established policies and procedures*. https://www.gao.gov/products/gao-19-105

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishing Group.

Kulko-Labyntseva, I. (2025). Security dynamics in the Black Sea region: Analyzing the intersection of NATO policies, Russian influence, and economic interests. Politics & Security, 12(2), 104–114. Doi: 10.54658/ps.28153324.2025.12.2.pp.104-114

SECURITY DYNAMICS IN THE BLACK SEA REGION: ANALYZING THE INTERSECTION OF NATO POLICIES, RUSSIAN INFLUENCE, AND ECONOMIC INTERESTS

Inna Kulko-Labyntseva
Pro-bisness outsourcing company
Legal Adviser
Ukraine
https://orcid.org/0000-0002-8491-0655

Abstract *The Black Sea has re-emerged as a central theater of geopolitical competition where NATO's defensive posture, Russia's revisionist ambitions, and the geoeconomics of energy and trade are locked in a complex, dynamic interplay. Russia's full-scale invasion of Ukraine has shattered the post-Cold War security architecture, creating a precarious new reality. This article analyzes the key drivers of instability, assesses the shifting balance of power, and evaluates strategic prospects. It argues that while Ukrainian asymmetric warfare has checked Russian naval dominance, the region remains acutely vulnerable to hybrid threats and escalation, demanding a more coherent, resourced, and integrated strategy from Western actors.*

Keywords Security policy, Black Sea, Russia, NATO.

1. INTRODUCTION

The Black Sea's enduring strategic importance is rooted in its geography as a maritime crossroads linking Europe, Asia, and the Middle East (Cambridge University Press, 2025; CSIS, 2025; Expedition Magazine, 2025). For millennia, it has been a contested space for empires, from the ancient Greeks, Romans, and Byzantines to the Ottomans and Russians, who fought twelve wars across four centuries largely for control of Crimea and the wider region (Cambridge University Press, 2025). The sea served as a terminus for the Silk Road and a vital source of grain, fish, and timber for the great Mediterranean empires, making it a center of international commerce and cultural exchange (Expedition Magazine, 2025). Throughout this long history, a consistent geopolitical truth has held: control of the Turkish Straits—the Bosphorus and the Dardanelles—is the key to regional dominance, granting or denying access between the Black Sea and the world's oceans (Britannica, 2025). This geographic chokepoint has been the subject of centuries of diplomatic maneuvering and conflict, from the Ottoman Empire's consolidation of control in 1453 to the great power rivalries of the 19th and 20th centuries (USNI Proceedings, 1952).

The dissolution of the Soviet Union in 1991 ushered in a period of relative tranquility, a historical anomaly that saw the Black Sea recede from the forefront of global security concerns (USIP, 2023). This era was marked by attempts to build cooperative frameworks, most notably the Black Sea Economic Cooperation (BSEC) organization, founded in 1992 with Turkish leadership to foster trade and dialogue among the littoral states (BSEC, 2022). However, this interregnum proved fragile and short-lived. The re-emergence of the Black Sea as a security hotspot began with Russia's 2008 war against Georgia and was cemented by Moscow's illegal annexation of Crimea in 2014 and its full-scale invasion of Ukraine in 2022 (USIP, 2023). These acts of aggression systematically dismantled the post-Cold War status quo, transforming the region from a secondary concern into a central theater of military conflict that directly threatens the security and stability of the entire Euro-Atlantic community (Cambridge University Press, 2025).

Today's security dynamics in the Black Sea are defined by the intense and volatile intersection of three primary forces. First is the collective security posture of the North Atlantic Treaty Organization (NATO), which seeks to deter aggression against its three littoral members—Bulgaria, Romania, and Turkey—while supporting its embattled partners, Ukraine and Georgia (NATO, 2023). Second are the revisionist ambitions of the Russian Federation. Moscow seeks to re-establish a dominant sphere of influence, roll back NATO's presence, and leverage the region as a critical springboard for projecting military and political power into the Mediterranean, Middle East, and Africa (U.S. Department of Defense, 2023). Third is the fierce geoeconomic competition over energy and trade. The region is both a critical conduit for global food supplies and an arena for competing energy transit corridors, pitting Russian-backed pipelines against Western-supported alternatives designed to enhance Europe's energy security (Cambridge University Press, 2025).

These overlapping and often conflicting dynamics are governed and constrained by a unique legal framework, principally the 1936 Montreux Convention Regarding the Regime of the Straits. This treaty grants Turkey sovereign control over the Straits but also codifies rules for passage, most critically by limiting the size, number, and duration of stay for naval vessels of non-littoral states (Britannica, 2025). The Convention is not merely a historical artifact; it is a central, active variable in the current conflict, profoundly shaping the military options available to both Russia and NATO and elevating Turkey's role as the indispensable guardian of the gate (Atlantic Council, 2022).

The convergence of these factors makes the Black Sea more than just a regional flashpoint; it is a microcosm of a fracturing global order. The conflict there is not simply a territorial dispute but a direct challenge to the foundational principles of the post-Cold War international system (Chatham House, 2023). It simultaneously tests the inviolability of borders through Russia's annexation of Crimea, the principle of freedom of navigation through its naval blockades, the laws of armed conflict through its deliberate targeting of civilian infrastructure, and the efficacy of collective security alliances through NATO's response (Cambridge University Press, 2025). The competition unfolds across multiple domains, involving not just conventional military force but also sophisticated hybrid warfare, economic coercion, and legal maneuvering around the Montreux Convention (RAND Corporation, 2023). Consequently, the Black Sea has become a laboratory where the rules, norms, and power dynamics of a new, more contested global era are being forged and fought over. The outcome of this struggle will have precedent-setting implications for other contested regions and for the future of international security architecture.

2. THE ALLIANCE'S EASTERN BULWARK: NATO'S EVOLVING BLACK SEA STRATEGY

The accession of Romania and Bulgaria to NATO in 2004 and 2007, respectively, fundamentally altered the strategic map of the Black Sea, extending the Alliance's eastern flank directly to its shores (Baranets, 2022). For the first decade of their membership, NATO's military posture in the region remained relatively light, focused more on integration and partnership than on hard deterrence. Russia's illegal annexation of Crimea in 2014 was a strategic watershed moment, compelling the Alliance to undertake a significant reinforcement of its southeastern flank (NATO, 2023).

At the 2016 Warsaw Summit, NATO leaders responded by establishing a Tailored Forward Presence (tFP) in the Black Sea region. This initiative was designed to be a defensive, proportionate, and adaptable response to Russia's growing military assertiveness (NATO, 2023). While distinct from the more robust enhanced Forward Presence (eFP) battlegroups deployed in the Baltic states and Poland, the tFP shared the same strategic objective: to signal Alliance resolve and deter aggression by demonstrating that an attack on one Ally would be met by forces from across the Alliance.

Following Russia's full-scale invasion of Ukraine in February 2022, NATO dramatically accelerated its force posture adjustments. In an extraordinary summit in March 2022, Allies agreed to establish four new multinational battlegroups in Bulgaria, Hungary, Romania, and Slovakia. This decision effectively doubled the number of battlegroups and extended a continuous forward military presence along the entirety of NATO's eastern flank, from the Baltic Sea in the north to the Black Sea in the south (Lutsevych & De Waal, 2023). The land component of this reinforced posture in the southeast is centered on the multinational framework brigade headquartered in Craiova, Romania, to which numerous Allies, including Italy, Poland, and Portugal, contribute forces (NATO, 2023). This land presence is complemented by enhanced air policing missions, with Allies like Canada and Italy augmenting the efforts of the Romanian and Bulgarian air forces, and a more persistent maritime presence (NATO, 2023).

For years, NATO and its regional allies have used joint military exercises as a primary tool for enhancing interoperability and signaling political resolve. Annual exercises such as Sea Breeze, co-hosted by the United States and Ukraine since 1997, and Sea Shield, led by Romania, have been staples of the regional security calendar (Brattberg & Sloat, 2023).

In the wake of the 2022 invasion, the focus and intensity of these drills have shifted decisively. They have evolved from partnership-building and confidence-building activities into complex, multi-domain operations designed to hone high-intensity warfighting skills. A clear example of this adaptation is the heightened focus on mine countermeasures (MCM). Russia's widespread use of sea mines has rendered large parts of the Black Sea unsafe for navigation, disrupting commerce and threatening civilian vessels (USIP, 2023). In response, exercises like Sea Breeze 25-2 have been specifically designed to improve collective capabilities in mine hunting, explosive ordnance disposal, and the use of unmanned underwater vehicles (Romanian Ministry of National Defense, 2024). This practical focus has yielded tangible results, most notably the establishment in 2024 of a joint Mine Countermeasures Task Group by the three littoral NATO allies: Turkey, Romania, and Bulgaria (Turkish Ministry of Defense, 2024). This initiative represents a significant step towards littoral-led security solutions, demonstrating a regional commitment to addressing shared threats directly.

A defining and unalterable feature of the Black Sea security environment is the 1936 Montreux Convention. The treaty grants Turkey full sovereignty over the Turkish Straits but imposes strict limitations on the passage of warships belonging to non-Black Sea states. These rules limit the aggregate tonnage of foreign naval vessels that can be in the Black Sea at any one time (45,000 tons), the tonnage of any single vessel (15,000 tons), and the duration of their stay (21 days) (Kucera, 2023). For a major naval power like the United States, these restrictions are profound; they preclude the deployment of an aircraft carrier and limit its presence to, for example, just three Arleigh Burke-class destroyers at once (U.S. Naval Institute, 2023).

Since February 2022, Turkey has invoked Article 19 of the Convention, which allows it to close the Straits to the warships of belligerent powers during wartime. Ankara has applied this impartially, preventing Russia from reinforcing its beleaguered Black Sea Fleet with vessels from its other fleets, but also blocking NATO allies from sending their warships into the Black Sea (Turkish Ministry of Foreign Affairs, 2023). This strict enforcement, while contributing to the de-escalation of a direct naval confrontation between NATO and Russia, effectively neutralizes NATO's overwhelming conventional maritime superiority.

This legal reality creates a powerful strategic dependency on the navies of the littoral allies. With external naval power severely constrained, NATO's ability to project force, protect sea lines of communication, and deter aggression in the maritime domain rests almost entirely on the shoulders of the Turkish, Romanian, and Bulgarian navies (Brattberg & Sloat, 2023). While Turkey possesses a large and modern fleet, the naval capabilities of Romania and Bulgaria have historically been limited and reliant on aging, Soviet-era platforms (IISS, 2023). This capability gap is not merely a local or national concern; it represents a critical vulnerability for the entire Alliance's deterrence and defense posture on its southeastern flank. This elevates the strategic importance of national modernization programs, such as Romania's planned acquisition of new corvettes and submarines, from domestic priorities to essential components of NATO's collective security (Romanian Ministry of National Defense, 2024). Consequently, U.S. and broader European support for the naval modernization of Romania and Bulgaria is not simply a matter of assistance but a strategic imperative to shore up a critical Alliance weakness (U.S. Naval Institute, 2023).

NATO's "Open Door" policy remains a cornerstone of its approach to the region. At the 2008 Bucharest Summit, the Alliance made the landmark declaration that Ukraine and Georgia "will become

NATO members," provided they meet the necessary requirements (NATO, 2008). This promise, while a powerful symbol of Euro-Atlantic solidarity, is also a primary driver of Russia's perception of threat and its aggressive actions to prevent further NATO enlargement into what it considers its historical sphere of influence (Charap & Shapiro, 2021).

Beyond political declarations, NATO provides significant practical support to both partners. The Comprehensive Assistance Package for Ukraine and the Substantial NATO-Georgia Package (SNGP) are the primary vehicles for this cooperation. These tailored programs are designed to strengthen defense institutions, enhance the interoperability of their armed forces with NATO standards, and support broader security sector reforms (NATO, 2023). Key initiatives under the SNGP include the NATO-Georgia Joint Training and Evaluation Centre (JTEC) in Tbilisi, which serves as a hub for multinational training and contributes to regional stability by improving the capabilities of Georgian forces (Kakachia & Lebanidze, 2020). Through these packages, NATO aims to bolster the resilience of its partners, enabling them to better defend themselves and continue on their path toward eventual membership.

3. THE REVISIONIST POWER: RUSSIAN AMBITIONS AND ACTIONS

The Kremlin's overarching strategic objective in the Black Sea is to transform it into a de facto "Russian Lake" or, at a minimum, a region where its military and political dominance is uncontested (Gorenburg, 2022). This ambition is not new but is a continuation of centuries of Russian imperial policy aimed at securing warm-water ports and projecting power southwards. In the contemporary context, this doctrine entails several core goals: establishing undisputed military supremacy, controlling key trade and energy corridors, preventing Ukraine and Georgia from integrating into Euro-Atlantic security structures like NATO, and using the region as a vital logistical and operational springboard for power projection into the Mediterranean, the Middle East, and Africa (Brattberg & Sloat, 2023). Russia's military intervention in Syria, for example, would have been logistically untenable without its naval bases and access through the Black Sea (Kozhanov, 2021).

To achieve these strategic aims, Russia has engaged in the systematic weaponization of geography through military force. The 2014 annexation of Crimea was the pivotal event in this strategy. By seizing the peninsula, Russia not only secured the home base of its Black Sea Fleet (BSF) in Sevastopol but also transformed Crimea into a formidable military fortress (Howard, 2023). It became a bastion saturated with advanced military hardware, including long-range air defense systems (S-400), anti-ship coastal missile batteries (Bastion), and a host of air and ground forces. This created a powerful Anti-Access/Area Denial (A2/AD) "bubble" that allowed Moscow to project force across the entire Black Sea basin and hold its neighbors at risk (Harding, 2023).

The 2022 full-scale invasion of Ukraine represented the violent culmination of this strategy. A primary military objective of the invasion was to conquer Ukraine's entire southern coastline, from Mariupol to Odesa. This would have achieved multiple strategic goals simultaneously: rendering Ukraine a landlocked and economically crippled state, creating a "land bridge" connecting mainland Russia to occupied Crimea, and extending Russian control westward to the border of Moldova's breakaway region of Transnistria, where Russian troops are already stationed (Brattberg & Sloat, 2023).

Parallel to its conventional military actions, Russia has waged a relentless and sophisticated hybrid war against the states of the Black Sea region (Giles, 2021). This multi-faceted campaign blends overt and covert instruments to destabilize societies, undermine governments, and weaken Western influence. Key components of this playbook include:

- Information and Cognitive Warfare: Russia deploys a vast and well-resourced propaganda and disinformation apparatus to manipulate public opinion. This "cognitive warfare" seeks to sow discord, erode trust in democratic institutions and Western alliances, promote anti-liberal and anti-Western narratives, and legitimize Russia's own aggressive actions (Giles, 2021). The 2008 war in Georgia served as an early and effective testing ground for these information warfare tactics, which have since been refined and scaled up (Pomerantsev, 2022).
- Economic Coercion: Energy has long been a primary weapon in Russia's arsenal. Moscow has repeatedly used its control over natural gas supplies to blackmail and exert political pressure on

dependent countries in the region, cutting off supplies or manipulating prices to achieve political ends (Mitrova & Yermakov, 2021).

- Cyberattacks: State-sponsored hacking groups conduct persistent cyberattacks against government websites, critical infrastructure, and financial institutions to disrupt economies and sow chaos (Giles, 2021).
- Exploitation of "Frozen Conflicts": Russia actively maintains and manipulates the "frozen conflicts" it helped create in the post-Soviet space. Its military presence in Georgia's breakaway regions of Abkhazia and South Ossetia, and in Moldova's Transnistria, provides Moscow with perpetual leverage, allowing it to destabilize these countries at will and effectively veto their Euro-Atlantic integration aspirations (Howard, 2023).

4. THE BLACK SEA FLEET: FROM ASSUMED SUPREMACY TO CONTESTED WATERS

At the outset of the 2022 invasion, Russia's Black Sea Fleet (BSF), having been significantly modernized in the preceding decade, was widely considered the dominant and uncontested naval power in the region (Gorenburg, 2023). However, the war has produced one of the most stunning naval upsets in modern history. Ukraine, a nation with a negligible conventional navy, has successfully challenged and neutralized this superior force through the innovative application of asymmetric warfare (Watling & Reynolds, 2023).

Leveraging a combination of domestically produced Neptune anti-ship missiles, which famously sank the BSF's flagship, the cruiser *Moskva*, in April 2022, and a growing fleet of sophisticated unmanned surface vehicles (USVs), or sea drones, Ukraine has inflicted devastating losses on the Russian fleet (Gorenburg, 2023). A significant portion of the BSF's warships have been sunk or severely damaged, forcing a fundamental change in Russian naval strategy. Ukraine's capabilities have effectively created a “sea denial” zone in the northwestern Black Sea. This has compelled the BSF to adopt a largely defensive posture, withdraw its most valuable assets from the vulnerable port of Sevastopol to the safer, more distant port of Novorossiysk, and largely cease offensive operations in the western part of the sea (Howard, 2023). The BSF's role has been relegated primarily to launching long-range *Kalibr* cruise missile strikes from the relative safety of the eastern Black Sea and protecting its own bases and infrastructure from Ukraine’s relentless drone attacks (Gorenburg, 2023).

These military setbacks at sea have had profound geopolitical consequences, inadvertently accelerating the very trends Russia’s aggression was meant to prevent. The Kremlin’s primary goal was to establish unchallenged dominance and halt Western integration and influence in the region (Brattberg & Sloat, 2023). However, its failure to secure control of the northwestern Black Sea and the severe degradation of its fleet created a power vacuum that other actors have rushed to fill (Watling & Reynolds, 2023). This enabled Ukraine to defy Russia’s blockade and establish its own “humanitarian corridor” for grain exports, restoring a vital economic lifeline and undermining Moscow’s attempts to weaponize global food supplies (World Bank, 2023). Furthermore, the demonstrated vulnerability of Russian naval power has emboldened regional actors. It has cemented Turkey’s position as the preeminent regional naval power and spurred NATO allies Romania and Bulgaria to accelerate the development of their own offshore energy projects, which are in direct competition with Russian gas exports (Kirişci, 2023). In effect, Russia’s tactical military failures have triggered a strategic blowback. By failing to create its desired “Russian Lake,” Moscow has unintentionally catalyzed the very outcomes—a more resilient and defiant Ukraine, stronger regional cooperation among its rivals, and a clearer path toward regional energy independence from Russia—that its war was designed to forestall.

5. THE GEOECONOMIC BATTLEGROUND: ENERGY, TRADE, AND INFRASTRUCTURE

The Black Sea region is a critical nexus for competing energy transit strategies, representing a geoeconomic battleground between Russia and the West. For decades, Russia has strategically promoted pipeline projects designed to bypass Ukraine, solidify its grip on the European energy market, and extend its political leverage. Key among these are the Blue Stream pipeline, operational since 2003, and the more recent TurkStream pipeline, both of which traverse the Black Sea to deliver Russian natural gas directly to Turkey and, from there, to Southern and Southeastern Europe (Mitrova & Yermakov, 2023). These projects were conceived not only as commercial ventures but as geopolitical tools to increase dependency on Gazprom and marginalize Ukraine as a transit state.

In direct opposition to this strategy, the European Union and the United States have backed the development of the Southern Gas Corridor (SGC). This monumental infrastructure project, consisting of the South Caucasus Pipeline (SCPX), the Trans-Anatolian Pipeline (TANAP), and the Trans-Adriatic Pipeline (TAP), is designed to transport Caspian gas from Azerbaijan through Georgia and Turkey into the European market (Umbach, 2022). The explicit strategic purpose of the SGC is to diversify Europe's energy supply, thereby reducing its vulnerability to Russian energy blackmail. This “pipeline race” is a clear manifestation of the broader geopolitical struggle for influence in the region.

Beyond transit routes, major offshore natural gas discoveries are poised to fundamentally reshape the regional energy map and further challenge Russia's dominance. The discovery and development of Turkey's massive Sakarya gas field (with estimated reserves of 540 billion cubic meters) and Romania's Neptun Deep field (around 100 bcm), along with Bulgaria’s potential Khan Asparuh field, promise to transform these nations from net energy importers to significant regional producers and exporters (Oktav, 2023).

These projects hold immense strategic significance. For Romania, Neptun Deep could make it the largest natural gas producer in the European Union, ensuring its own energy independence and allowing it to export to neighbors like Moldova, Hungary, and Austria. For Turkey, the Sakarya field will drastically reduce its heavy dependence on Russian gas imports. For Bulgaria, developing its offshore reserves would secure its domestic consumption and turn it into an exporter. Because these indigenous energy sources directly compete with Russia's economic and political interests, the offshore platforms, pipelines, and exploration vessels associated with them are considered high-risk targets for Russian hybrid interference, including naval harassment, GPS jamming, and potential sabotage (Brattberg & Sloat, 2023).

Table1: Tangible nature of the energy competition

Project Name	Type	Key Stakeholders	Status	Capacity/Reserves	Strategic Significance
TurkStream	Gas Pipeline	Russia (Gazprom), Turkey (BOTAŞ)	Operational	31.5 bcm/year	Bypasses Ukraine; solidifies Russian supply to Turkey & SE Europe.
Blue Stream	Gas Pipeline	Russia (Gazprom), Italy (Eni), Turkey	Operational	16 bcm/year	Diversified Russian export route to Turkey, predating TurkStream.
Southern Gas Corridor (TANAP/TAP)	Gas Pipeline	Azerbaijan (SOCAR), Turkey, BP, EU	Operational	16 bcm/year (expandable)	Key non-Russian supply route to Europe; enhances Turkey's transit role.
Neptun Deep	Offshore Gas Field	Romania (OMV Petrom, Romgaz)	Development	~100 bcm	Will make Romania largest EU gas producer; enables regional exports.
Sakarya	Offshore Gas Field	Turkey (TPAO)	Production started	~540 bcm	Drastically reduces Turkey's import dependency, especially on Russia.
Khan Asparuh	Offshore Gas Field	Bulgaria (OMV Petrom)	Exploration	~60 bcm	Potential to make Bulgaria energy self-sufficient and an exporter.

This data illustrates the tangible nature of the energy competition. The significant reserves of fields like Sakarya and Neptun Deep represent a long-term structural shift away from dependence on Russian pipeline gas. The operational status of TurkStream and the Southern Gas Corridor highlights the parallel infrastructure networks that define the region's energy politics. The "Strategic Significance" column translates this technical data into direct geopolitical impact, clarifying the stakes for regional and global actors. This juxtaposition makes the abstract concept of a "pipeline race" concrete, showcasing a geoeconomic landscape in profound transition.

6. THE GLOBAL BREADBASKET UNDER SIEGE

The Black Sea is a vital artery for global food supplies. Russia and Ukraine are among the world's top exporters of wheat, corn, barley, and sunflower oil, with dozens of countries in the Middle East and Africa critically dependent on these shipments for their food security (Dandashly & Öztürk, 2023). Russia has systematically weaponized this dependency as part of its war effort. Its naval blockade of Ukraine's ports, deliberate missile strikes on grain terminals and agricultural infrastructure, and temporary withdrawal from the UN-brokered Black Sea Grain Initiative were all calculated actions designed to cripple Ukraine's economy, create global food shortages and price spikes, and generate political instability in import-dependent nations (Mitrova & Yermakov, 2023).

A major strategic success for Ukraine and its partners has been the establishment of a "humanitarian corridor" in August 2023. This shipping lane hugs the coastlines of NATO members Romania, Bulgaria, and Turkey, using their territorial waters as a shield against Russian interdiction. This corridor has proven remarkably effective, allowing Ukraine to restore its grain exports to near pre-war levels and demonstrating the practical limits of Russia's naval blockade in the face of determined regional cooperation (Brattberg & Sloat, 2023).

The war has starkly illuminated the extreme vulnerability of the region's critical infrastructure. This extends beyond ports and grain silos to include offshore energy platforms, subsea gas pipelines, and underwater fiber-optic data cables. These assets have become legitimate targets in a multi-domain conflict. They are vulnerable to both direct kinetic strikes from missiles and drones—as evidenced by attacks on Ukrainian port facilities and the Tavrida drilling rig—and to more insidious hybrid attacks, such as cyber intrusions, GPS spoofing and jamming, and covert sabotage by special forces or unmanned underwater vehicles (Umbach, 2022). The targeting of this infrastructure poses a severe risk of economic disruption and environmental disaster and represents a dangerous rung on the escalation ladder.

7. CASE STUDIES IN REGIONAL SECURITY DYNAMICS

7.1 UKRAINE: THE CRUCIBLE OF CONFLICT AND ASYMMETRIC INNOVATION

Ukraine stands as the undeniable epicenter of the Black Sea conflict. Its national survival and sovereignty are at stake, and its resistance has reshaped the regional and global security landscape. The defining feature of Ukraine's military effort has been its remarkable success in asymmetric naval innovation. Facing a vastly superior Russian navy, Ukraine leveraged ingenuity and Western-supplied technology to develop and deploy a formidable arsenal of anti-ship missiles and, most notably, unmanned surface vehicles (USVs). These "sea drones" have proven to be a cost-effective and highly lethal tool, capable of overwhelming the defenses of large warships (Gorenburg, 2023). This strategy has not only inflicted crippling losses on the Russian Black Sea Fleet but also provided a powerful case study in modern naval warfare, with global implications for how smaller nations can counter larger maritime powers (Herpen, 2023). Beyond its military successes, Ukraine's ability to establish and maintain a grain export corridor, in cooperation with its neighbors, demonstrates its strategic acumen and resilience, ensuring its economic viability and mitigating Russia's attempts to weaponize food (Mitrova & Yermakov, 2023). The future trajectory of Ukraine is the single most critical variable determining the long-term security architecture of the entire Black Sea region (Sloan, 2022).

7.2 TURKEY: THE INDISPENSABLE BALANCER AND GUARDIAN OF THE STRAITS

Turkey's role in the Black Sea is uniquely complex and pivotal. It navigates a multifaceted balancing act, simultaneously acting as a committed NATO ally, an ambitious regional power, a cautious rival to Russia, and a crucial economic and diplomatic partner to both sides (Brattberg & Sloat, 2023). Ankara has armed Ukraine with critical weaponry like Bayraktar drones while refusing to join Western sanctions against Russia (Candar, 2023). This policy is underpinned by its strict and impartial enforcement of the Montreux Convention, a position that both contains Russian naval reinforcements and limits NATO's direct maritime presence, thereby preserving Turkey's central role as the gatekeeper of the Black Sea (Umbach, 2022).

Ankara's foreign policy is increasingly driven by a desire for strategic autonomy, articulated through concepts like the "Blue Homeland" (*Mavi Vatan*) doctrine, which calls for a more assertive naval presence to protect its maritime interests (Herpen, 2023). The significant degradation of Russia's Black Sea Fleet has, by default, made Turkey the undisputed strongest naval power in the region, further enhancing its strategic weight (Gorenburg, 2023). Its indispensable role in energy transit (hosting both TurkStream and the Southern Gas Corridor) and its leadership in regional security initiatives, like the trilateral Mine Countermeasures Task Force with Romania and Bulgaria, make it an unavoidable and essential player in any future security arrangement (Yermakov, 2023).

7.3 ROMANIA & BULGARIA: NATO'S FRONTLINE STATES AND EMERGING ENERGY PLAYERS

As the only EU members with Black Sea coastlines besides Turkey, Romania and Bulgaria are frontline states in the confrontation with Russia. They are central to NATO's deterrence posture, hosting multinational battlegroups, key air bases like Mihail Kogălniceanu, and other critical Alliance infrastructure (NATO, 2023). The war has thrust them into a new strategic role as vital logistical hubs for supporting Ukraine. Romania's port of Constanța, in particular, has become the primary gateway for diverted Ukrainian grain exports, handling a massive volume of trade that was previously shipped from Odesa and other ports (Umbach, 2022).

Beyond their military and logistical importance, both countries are on the cusp of becoming significant European energy producers. The development of Romania's Neptun Deep and Bulgaria's potential Khan Asparuh offshore gas fields will not only secure their own energy independence but has the potential to turn them into key suppliers for the wider region, offering a concrete alternative to Russian gas (Mitrova & Yermakov, 2023). This rising geoeconomic profile is matched by a growing security assertiveness, reflected in joint initiatives like the establishment of a Regional Special Operations Command (HQ R-SOCC) (Gorenburg, 2023). However, both nations remain vulnerable to Russia's hybrid warfare tactics and face challenges related to internal political fragility and corruption (Koval, 2023).

7.4 GEORGIA: THE ENDURING LEGACY OF "FROZEN CONFLICT" AND EURO-ATLANTIC ASPIRATION

Georgia's experience serves as a stark case study of Russia's long-term strategy for maintaining regional control. The 2008 Russo-Georgian War and Russia's subsequent recognition and military occupation of the breakaway regions of Abkhazia and South Ossetia established a "frozen conflict" on Georgian soil (Herpen, 2023). This has proven to be a highly effective tool for Moscow, creating a state of perpetual instability that allows it to exert leverage over Tbilisi and effectively block Georgia's path to NATO membership, as the Alliance is reluctant to admit new members with unresolved territorial disputes.

Despite overwhelming public support for integration with the EU and NATO, Georgia faces immense and continuous pressure from Russian hybrid warfare. This includes pervasive disinformation campaigns, economic leverage, and political subversion aimed at eroding democratic institutions and fostering pro-Russian sentiment (Sloan, 2022). These efforts have contributed to a significant democratic backslide in recent years, with the government adopting policies that have strained relations with Western partners and led to a suspension of its EU accession process (Koval, 2023). Russia's recently announced plans to establish a permanent naval base in Abkhazia represent a further escalation, threatening to cement its military footprint and project power further along the eastern Black Sea coast (Umbach, 2022).

8. CONCLUSION

The security landscape of the Black Sea has been fundamentally and irrevocably altered. The pre-2022 balance of power, which was characterized by Russia's clear military dominance and a relatively passive

Western posture, is broken. In its place, a new, more fluid, and intensely contested equilibrium has emerged (Candar, 2023).

Militarily, Russia's formidable land and air power in the region remains a potent threat, but its naval supremacy has been decisively checked by Ukraine's asymmetric capabilities. Turkey has emerged as the preeminent regional naval power, while NATO's land-based deterrence on its eastern flank has been significantly bolstered. However, the Alliance's ability to project maritime power remains severely constrained by the Montreux Convention (Brattberg & Sloat, 2023).

Economically, Russia's once-powerful energy leverage over Europe has been drastically curtailed. The rise of new regional energy producers like Romania and Turkey, coupled with the development of alternative transit routes such as the Middle Corridor, points toward a more diversified and resilient regional energy future. This emerging infrastructure, however, is itself a new and attractive target for Russian aggression (Mitrova & Yermakov, 2023).

Politically, the war has solidified a pro-Western bloc led by a defiant Ukraine and supported by frontline allies like Romania. Simultaneously, it has highlighted the complex and transactional balancing act of Turkey and exposed the acute vulnerabilities of Georgia and Moldova to sustained Russian political and hybrid pressure (Sloan, 2022).

The most immediate and probable danger in the Black Sea is not necessarily a direct, all-out war between NATO and Russia, but rather a series of deliberate escalatory steps within the "grey zone" of conflict, below the threshold of conventional warfare (Sloan, 2022). The primary risks on this escalation ladder include:

1. Attacks on Critical Infrastructure: The highest risk involves Russian hybrid or kinetic strikes against the region's emerging energy architecture. Sabotaging offshore gas platforms, subsea pipelines, or underwater data cables would be a calculated move to disrupt the region's economic diversification away from Russia, create economic chaos, and test Western resolve (Umbach, 2022).
2. Miscalculation at Sea or in the Air: The increased tempo of NATO surveillance flights and Russian military patrols creates a heightened risk of accidental or deliberate clashes between opposing forces, which could spiral into a wider crisis (Sloan, 2022).
3. Horizontal Escalation: Faced with a stalemate in Ukraine, Russia may be tempted to open a new front or create a diversion by escalating its pressure on more vulnerable states. This could involve engineering a crisis in Moldova via its proxies in Transnistria or further destabilizing Georgia to distract and divide Western attention (Umbach, 2022).
4. Vertical Escalation: While remote, the possibility of Russia using a low-yield tactical nuclear weapon to "de-escalate" a conventional conflict in which it faces catastrophic defeat cannot be entirely dismissed. Such an act, intended to shock and awe adversaries into submission, represents the highest rung of the escalation ladder (Sloan, 2022).

Navigating this perilous environment and fostering long-term stability requires a coherent, well-resourced, and unified strategy from the United States and its European allies. The current EU strategy, while well-intentioned, has been criticized as being largely declarative and lacking the concrete action plans and dedicated funding needed for meaningful impact (Brattberg & Sloat, 2023). An effective approach must be built on three pillars:

First, strengthening multilateral cooperation among littoral allies is paramount. The constraints of the Montreux Convention make regional, self-sustaining security formats essential. The West should actively support and seek to expand initiatives like the Turkish-Romanian-Bulgarian Mine Countermeasures Task Force and the Regional Special Operations Command (Rácz, 2022). These formats, led by the allies most directly affected, are the most credible and sustainable vehicles for ensuring maritime security.

Second, the West must commit to bolstering the resilience of frontline and partner states. This requires sustained investment in the naval and integrated air and missile defense capabilities of Romania and Bulgaria to create a credible regional deterrent. It also means continuing to provide Ukraine with the advanced weaponry it needs to maintain sea denial against the Russian fleet and protect its economic lifelines. Simultaneously, a robust strategy must be deployed to counter Russian disinformation and support democratic institutions in Georgia and Moldova, hardening them against political subversion (Koval, 2023).

Finally, it is crucial to recognize that a truly stable Black Sea is impossible as long as Russia illegally occupies Ukrainian territory. A frozen conflict, with Russia retaining control of Crimea and other coastal areas, would guarantee perpetual instability, as Moscow would continue to use these territories as platforms for aggression and malign influence (Sloan, 2022). Therefore, the future security of the region is inextricably linked to the outcome of the war in Ukraine. A Ukrainian victory that restores its sovereignty over its internationally recognized 1991 borders, including Crimea, would dismantle Russia's primary power projection platform and represents the most durable path toward a secure, stable, and prosperous Black Sea region anchored in the Euro-Atlantic community (Koval, 2023).

REFERENCES

Aydın, M. (2025). *Turkey's Black Sea policies (1991–2023) and changing regional security since the Russian invasion of Ukraine*. ResearchGate. https://www.researchgate.net/publication/376185529

Bechev, D. (2025). *Bridging the Bosphorus: How Europe and Turkey can turn tiffs into tactics in the Black Sea*. European Council on Foreign Relations. https://ecfr.eu/publication/bridging-the-bosphorus/

Chitadze, N. (2025). *The hybrid war waged by the Russian Federation in the Black Sea region in the format of information-psychological operations on the example of Georgia*. ResearchGate. https://www.researchgate.net/publication/378812013

Chitadze, N., Vdovychenko, V., & Albu, N. (2024). *Russia-Ukraine war and geopolitical competition in the Black Sea region*. European Neighbourhood Council. https://www.encouncil.org/russia-ukraine-blacksea

Council of the European Union. (2025). *EU strategic approach Black Sea strategy*. https://data.consilium.europa.eu/doc/document/ST-7773-2025-INIT/en/pdf

CSD (Center for the Study of Democracy). (2024). *Countering hybrid warfare in the Black Sea region*. https://csd.bg/publications

Ditrych, O. (2024). *Four swans of the Black Sea*. European Union Institute for Security Studies. https://www.iss.europa.eu/content/four-swans-black-sea

German Marshall Fund of the United States (GMFUS). (2025). *EU's new Black Sea security strategy: Right goals, unclear means*. https://www.gmfus.org/news/eus-black-sea-strategy

Harangozo, T. (2025). *The war in Ukraine and mounting economic challenges in the greater Black Sea region*. NATO Parliamentary Assembly. https://www.nato-pa.int/document/war-ukraine-and-economic-challenges

Iancu, G., & Stoicescu, E. (2024). *Offshore energy potential in the Black Sea*. New Strategy Center. https://newstrategycenter.ro/publications

Lancaster, M. (2023). *Black Sea security after Russia's invasion of Ukraine*. NATO Parliamentary Assembly. https://www.nato-pa.int/document/black-sea-security-2023

Larsen, R. (2024). *A security strategy for the Black Sea*. Atlantic Council. https://www.atlanticcouncil.org/black-sea-strategy

Mercy Corps. (2023). *Potential impact of Black Sea escalations on food security in the Middle East and North Africa*. https://www.mercycorps.org/research-resources/black-sea-food-security

Murphy, M., & Schaub, G., Jr. (2018). "Sea of peace" or sea of war—Russian maritime hybrid warfare in the Baltic Sea. *Naval War College Review, 71*(2), Article 9. https://digital-commons.usnwc.edu/nwc-review/vol71/iss2/9

NATO. (2025). *NATO's forward land forces*. https://www.nato.int/cps/en/natohq/topics_136388.htm

Pop, I. (2025). *Romania's emerging role in NATO's eastern flank: Infrastructure, industry, and strategic commitments*. China-CEE Institute. https://china-cee.eu/policy-brief-romania-in-nato

Stronski, P. (2021). *What is Russia doing in the Black Sea?* Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/11/04/what-is-russia-doing-in-black-sea-pub-85687

Tarasov, I. (2024). *The transformation of the Black Sea into a Russian lake*. Italian Association of Russian and Eurasian Studies (IARI). https://www.iari.site/2024/03/11/the-russian-lake/

Tessier, L. (2024). *Russia's Black Sea Fleet in the special military operation in Ukraine*. Foreign Policy Research Institute. https://www.fpri.org/article/2024/01/russias-black-sea-fleet/

U.S. Congress. (2023). *S.804 - Black Sea Security Act of 2023*. https://www.congress.gov/bill/118th-congress/senate-bill/804

Wallander, C. (2024). *What you need to know about security in the Black Sea*. Johns Hopkins SAIS. https://sais.jhu.edu/news-press/security-black-sea

Yilmaz, S. (2023). Türkiye's Black Sea policy for energy security. *Vestnik RUDN. International Relations, 23*(4), 748–761. https://journals.rudn.ru/international-relations/article/view/37277