The Impact of International Sanctions on Ukraine's Sustainable Development in the Context of Russian Cyberwarfare

Petro Korniienko[1], Iaroslav Petrunenko[2]

Received: 16.02.2023
Accepted: 02.05.2023
Published: 25.05.2023

Abstract. Ukraine's sustainable development has been profoundly affected by Russia's continuing international sanctions especially in relation to the increased use of cyber warfare by Russia. There are many effects of the sanctions such as loss of supply chains, low foreign direct investment, and enhancement of the levels of threat to the country's cyberspace, the research states. The study does look into this structural and economic problem from several angles, including: challenging the microeconomics of the problem: the exchange of information among the players involved, the potential economic gain that is prevented, the wasted economic gain, the cut-off supply lines, etc. Real-world data, policy review and interviews with relevant parties indicate that these are issues of, amongst others, trade network breakdown, flight of foreign investment and rise in cyber insecurity. Also, it looked at the relationship between the sanctions imposed and the threats posed by cyber warfare and how these two elements make Ukraine's sustainability processes painstakingly long. The findings underscore the need for a proactive intervention plan severely fortified by cyber security strategies. This underlines the need for Ukraine to employ a comprehensive approach where both the short term strategies aimed at countering sanctions and the broader threat of cyber warfare are designed to support economic expansion, as effective within the given limitations.

Keywords: economic resilience, cyber threats, supply chain disruptions, investment climate, security strategies.

INTRODUCTION

The enduring situation in Ukraine alongside most of the Russian elements, cyberwarfare being one, is a tall order towards the sustenance of development. With the pursuit of mending the economic imbalance restored to the world, Ukraine has to deal with external challenges such as how to fight against cyberattacks especially when it is under sanctions. While global measures are put in place to curb the offending behavior of states, such restrictions have always been known to have effects on the economy of those states affected by them. In the instance of Ukraine, these sanctions have taken place against the persistent cyberattacks that have been focused on destabilizing its infrastructure and governance thereby necessitating an intricate scrutiny on how they have jointly affected its developmental path.

People generally employ the term "international sanctions" to refer to the mechanisms contained someone's preferences in developed countries penetration trade, investment, and financial system (such as capital

[1] Petro Korniienko
Dr. hab in Law, Professor, Department of Philosophy, Law and Social-Humanitarian Disciplines, Faculty of Finance and Economics, National Academy of Statistics, Accounting and Audit, Kyiv, Ukraine, petrokorniienko@nasaa.edu.ua, https://orcid.org/0000-0002-1473-6698
[2] Iaroslav Petrunenko
Doctor of Juridical Science, Full Professor, Senior Researcher, State Organization «V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine», Kyiv, Ukraine, petrunenko@yahoo.com, https://orcid.org/0000-0002-1186-730X

flight from developing countries). While the objectives of such measures may include defending against hostile attacks or coercing individuals into certain actions, enough research has not been done to ascertain how they impact a country's development particularly when it comes to persistent conflicts (Herbert, 2022; Jones & Whitworth, 2014). In regard to Ukraine, the imposition of sanctions led to economic stagnation hence depriving it of its' potential growth and basic needs (Orakhelashvili, 2015; Simonen, 2015). Also, these sanctions often bring about unexpected results. For example, civilians tend to suffer more while there are difficulties in rebuilding crucial infrastructure (Boloukian, 2016; Shkrabak, 2020).

Sustainable development in Ukraine is made more complex by cyber warfare. Through cyber warfare, critical services can be paralyzed, security systems can be hacked leading to low public trust (Gupta & Rao, n.d.; Putra, 2022). This undermines immediate responses to conflicts and has far-reaching economic consequences as well as unstable social relations. The above challenges show the need for a comprehensive regulatory framework that is strong enough so as to be able to handle emergent effects of imposition of sanctions as well as ongoing challenges posed by cyber activities.

Also, capricious regulatory policies or penalties serve as stumbling blocks in responding to abrupt worldwide occurrences (Ivanova, 2015; Semenenko, Halhash, & Ivchenko, 2019). In this context, does it fit into the Sustainable Development Goals to define the perplexing ways in which these exacerbate recovery and resilience-building efforts in Ukraine? Moreover, the issue becomes harder still because of other pressing enquiries such as what strategies Ukraine would use to recover from calamities and grow amid looming threats of cyber-attacks that call for immediate solutions? Additionally, the balance between progressing economically and remaining secure as a nation poses a dilemma as far as rapid growth is concerned in this country.

Research Problem

Ukraine's efforts to achieve a sustainable development trajectory are thwarted by cybersecurity measures that are no longer functional and rigid international regulations. These prescriptions lack coherence, they do not have any identifiable thresholds which regulate allowance vis-a -vis economic regulations and cyber terrorism as opposed to the overall safety of the nation (Lopez & Cortright, 2018; The impact of us economic sanctions on russia's social-economic development, 2019). Unethical long-term effects are manifested through some strange sanctions levied against the Ukrainian economy;its vital infrastructure does not have cyber attack protection or any viable and targeted anti-economic punishment measures. This implies that Ukraine will be unable to achieve any desired development goal as all these issues have bred strong relationship with each other thereby weakening it in the wake of emerging geopolitical rifts.

Moreover, it is important to remember that international sanctions and cyber warfare have an impact on human life. Limited economic access tends to worsen current weaknesses thus aggravating cases of increased poverty and social dissatisfaction according to various studies (Haminskiy, 2021; Rusinova et al., 2020). In addition, necessary services like medical care and education among others can fail through cyberattacks leading to a further breakdown of the moral fiber that holds communities together. In this context, Ukraine is faced with two opposing forces but they are both similar meaning it fails to progress efficiently thus causing the country's leaders relook policy at globally and within their boundaries immediately.

Research Focus

The proposed research aims to assess the impact of international sanctions and Russian cyberwarfare on Ukraine's sustainability trajectory.

Emphasis will be put on three dimensions in particular:

1. There has to be an evaluation made to look into how the economic sanctions have performed within an economy, the sectors that can be invested in all, and the level of provision of basic needs in Ukraine so as to help assess the direct and indirect impacts of economic restrictions on the economy of Ukraine for the path of sustainable development.

2. It is noteworthy that there is a lot to be desired in the understanding of how cyber assaults create a situation whereby some sanctions imposed on Ukraine give it more challenges. Examples are also drawn on the cyber attack on critical infrastructures and their role in the country's defense.

3. Suggesting optimal policy recommendations that will help in fully applying sanctions against the aggressors, while at the same time, promoting effective recovery and development of Ukraine. This might assist in the institutionalization of a holistic approach which considers both national security issues and the need to meet developmental objectives.

Nonetheless, there is an urgent difficulty in coming up with and enforcing a well-rounded strategy that connects the concerns of international sanctions and national cyber security as well as sustainable development. The research examines the case of the conflict in providing useful information so as to address the current threats to security and the cause of development in the future with the aim of achieving peace and sustainable development in the area.

LITERATURE REVIEW

The ongoing struggle in Ukraine against Russia has led to the empowerment of the universities' research agenda with aspects of cybersecurity and sustainable development, as well as international sanctions whose combinations have always been of great concern. In this paper, the author examines a number of studies on the effects of global sanctions on different countries, as well as the effects of cyber warfare on the development of Ukraine, highlighting how these problems are interconnected.

For reasons such as seeking to influence those countries that are deemed to have violated any universal laws by changing their behavior, nations and global bodies frequently declare and enforce global sanctions. It is maintained that such policies on the contrary have devastating effects on the economy, the inflow of foreign direct investments snakes back and poverty rates soar in the affected countries (Economic sanctions reconsidered, 2008 Consolidated notation; Hufbauer, 2007). In the instance of Ukraine for example, when the Western nations applied sanctions to Russia, it was because of the latter's unprovoked hostility that went on to make significant barriers of trade, which as a result broke those economic and financial relations (Diachenko, 2022; Savinova, 2019).

These sanctions create an economic isolation that complicates recovery efforts in the short run and thwarts long term sustainable development goals by worsening pre-existing weaknesses in the Ukrainian economy. Sanctions can hinder the achievement of the UN Sustainable Development Goals (SDGs) through restricting access to basic services and aggravating humanitarian crises (Jessen, 2020). In Ukraine, these effects are more pronounced because there is an increase in joblessness as well as high prices leading people into revolts besides making governments less effective (Al-Samarrai, 2018; Cortright & Lopez, 2018).

In instances where an economy is in the doldrums, the ability of the administration to avail amenities and promotion of ideas shrinks, thus causing a negative feedback loop that deepens poverty as well as chaos in the long run (Rivera, 2010). This cycle serves as a good example on how not only can privileges prevent quick restoration of the economy, but also the larger society collapse that ensures development for all.

Moreover, Russian cyber aggression has escalated with the conflict initiation rendering the situation more intricate. Consequently, there is an increased incidence of cyber terrorism where critical infrastructures as well as government establishments suffer attacks while disrupting vital services thereby reducing trust levels (Averre & Wolczuk, 2018; Kenney, 2015). Cyber operations can worsen sanction effects due to compromising institutional trust and hampering economic rehabilitation efforts (Cyber warfare, 2017; Relia, 2015).

It is noted that the existing frameworks find it hard to deal with effectively economic sanctions and cyber threats that pose dual challenges (Lopez & Cortright, 2018; The impact of us economic sanctions on russia's social-economic development, 2019). The regulatory environment around sanctions and cybersecurity though is usually fragmented and inconsistent thereby lacking coherence or adaptability when the geopolitical landscape changes quickly. Multiple advantages of cyber warfare in the long run may make it difficult to assess its effectiveness due to its negative effects on economic stability and required developments costs.

Ukrainian rebuilding is currently made difficult by security and growth concerns. However, the problem can be addressed by a more coherent regulatory framework that would enable the country to survive in a passionate manner even under sanctions and cyber-attacks.

It is necessary to consider the humanitarian consequences of the restrictions together with cyberspace warfare and to see their broader societal implications. Sanctions are known to create more requirements for humanitarian assistance when there is no or limited access to health care, education or other vital services (especially in Ukraine) in areas affected by conflict (Haminskiy, 2021; Rusinova et al., 2020). Moreover, cyber-attacks often entail system failure which makes populations lose faith in their governments even more (Hansel et al., 2018; Hryshchuk & Tagarev, 2018).

Responses to dual pressure would require both local and international stakeholders to act in urgency and collaborate. Clearly, there is need for conflict policies that place emphasis on human rights and People's living standards because effects of cyber warfare disruption have been heightened by human suffering caused by economic sanctions.

Importantly, one other issue that is notable in the literature is the regulatory challenges surrounding sanctions as well as cybersecurity. It is crucial to have well defined laws that would effectively deal with cyber-activity difficulties peculiar to itself yet capable of performing sanctions simultaneously (Ganiev et al., 2018; Shin et al., 2016). Diverse regulatory factors among different countries exacerbate compliance problem with making it hard to follow and apprehend illegal activities (Bechara & Schuch, 2020; DiStaso, 2018).

This inconsistency prevents Ukraine from being fully compliant with the global system, leading to protectionism tendencies (Jaeger, 2018a; Jaeger, 2018b). Consequently, taxing digital asset transactions is closely related to both cyber wars and sanctions, setting up barriers for regulation and assisting in implementing sanctions as well as executing cyber attacks. Different jurisdictions have different ways of treating taxes on crypto assets, which leads to confusion among entrepreneurs and investors, makes it difficult for compliance to be achieved or creates opportunities for evasion (Dmitrieva, 2019; Shamraev, 2021).

In addition, broadly incorporating all aspects within cybersecurity towards Ukraine is emphasized in writing. The World Bank calls for extensive strategies encompassing economic recovery, security and sustainable development to foster resilience in conflict- affected areas (World bank group - international development, poverty, & sustainability, n.d.). Such an understanding supports (buttresses) demands for stronger cyber security frameworks that protect except/save critical infrastructure but also build/equip local economic development efforts capable of withstanding cyber threats.

There are critical questions concerning the future effectiveness of rehabilitation efforts in Ukraine in the light of the growing intersection between global sanctions, cyberwar and sustainable development. As the conflict transforms, grasping the interrelatedness of these matters becomes crucial for policy-makers. The need for merging economic recovery, security and sustainable development in order to enhance resilience of regions affected by wars has been proved by research (World bank group - international development, poverty, & sustainability, n.d.).

In order for Ukraine to meet its development goals and establish a viable future, it will have to manage international restrictions and cyber warfare. To put it differently, literature shows that international sanctions, cyber warfare and sustainable development in Ukraine are all intertwined.

Thought substantial number of research have been conducted on these topics separately, there is urgent need for a combined study on them and responded to within a single framework without further delay because of time gap between now and then. It is important to take into consideration that Ukraine's policies have compound nature which lead to her growth especially in times like these where there are constant political turmoil in the country. The shift in status quo require the use of more scientific researches that could address ways in which Ukraine should move away from the current predicaments.

RESEARCH METHODOLOGY

General Background

The issue of the multifaceted nature of how international sanctions alongside Russian cyber warfare may be dragging on Ukraine's sustainable growth needs to be thoroughly looked into. This paper aims to analyze how these elements interact in constructing the socio-economic environment. This facilitate an understanding of the complexities associated with the struggle of Ukraine – to achieve self-

sufficiency in such circumstances – through the application of mixed methodologies.

Methodological Approach

For the purposes of this analysis, the Authors combine qualitative and quantitative approaches to understand the interplay and complexity of international sanctions, cyberwarfare, and sustainable development. The methodology allows for the analysis of the psychological aspect and the feeling of those who are impact by these sanctions and cyber actions in addition to the quantitative effect of those sanctions and cyber actions.

In order to ensure that the research is of high quality and that political and regional biases during data collection are kept to a minimum, several measures were carefully taken. Positive, more stress was placed on organizational diversity by including recent journals, publications of international agencies, and many others in order to provide a better picture and avoid over-reliance on one region. Data triangulation, in this case, meant verifying the determined facts with Kaniv pro-Ukrainian sources and the neutral ones when discrepancies were reported. Also, efforts were made to collect honest responses from interviews and surveys with economists and policymakers, which were conducted by imposing the need for anonymity and confidentiality, which prevented punitive actions concerning the collected data. The sampling design employed was stratified sampling in the sense that it included all the regions of Ukraine in the study in order to lessen any regional turbulence in economic perceptions. Some reviewers who had no vested interests in the outcome of the research were sought from different professions and political standings to provide as much neutrality as possible to the research design and the findings. Last but not least, they all remained reflexive, leaning towards the data analysis process in a way that reflecting upon their preconceived ideas helped to make the analysis process more objective. Such strategies were intended to facilitate a sound and unbiased investigation of the issues connecting international sanctions, cyber warfare, and Ukraine's sustainable growth.

Quantitative Methods

The quantitative research in Ukraine is directed towards searching for the statistical links between global sanctions, incidences of cyber warfare, and parameters of sustainable development. Some main factors like the gross domestic product growth rate, the net foreign direct investments (FDI) amount, and some social indicators such as poverty level or employment rate will be analyzed using regression models. The research data will be sourced from appropriate databases recommended by the World Bank and national statistics agencies in order to ensure that we can trace long-term trends established.

In this research, linear regression as well as multivariate regression analysis will be conducted with aid of packages such as R and SPSS. Consequently, sanctions and cyber activities effect on Ukraine economic growth and social development can be measured by using these models which provide data for this study.

The qualitative analysis will consist of in-depth interviews that will unpack the lived experiences of people in organizations touched by international sanctions and cyber warfare. The participants will be selected using purposive sampling to ensure representation from all sides of government, industry, civil society and affected people.

The interviews will be partially structured to allow for flexibility in discussions but to also ensure that key issues are tackled in them. They will be recorded, transcribed, and analyzed using NVivo software for coding and thematic analysis. It is hoped that this approach will provide a more profound insight into the social-political, financial impacts that sanctions and cyber warfare has on sustainable growth within Ukraine.

Sample and Participants

In this research, 250 respondents in total are assigned into four categories. Each category corresponds to an important strategic element that shapes economic policy as well as the society. This way, government representatives, industry leaders, civil society representatives, and academics look at the issues at hand from different perspectives. The picture shows the percentage of the respondents in each of the given categories thus helping in appreciating the role of each category of respondents in the research study (Figure 1).

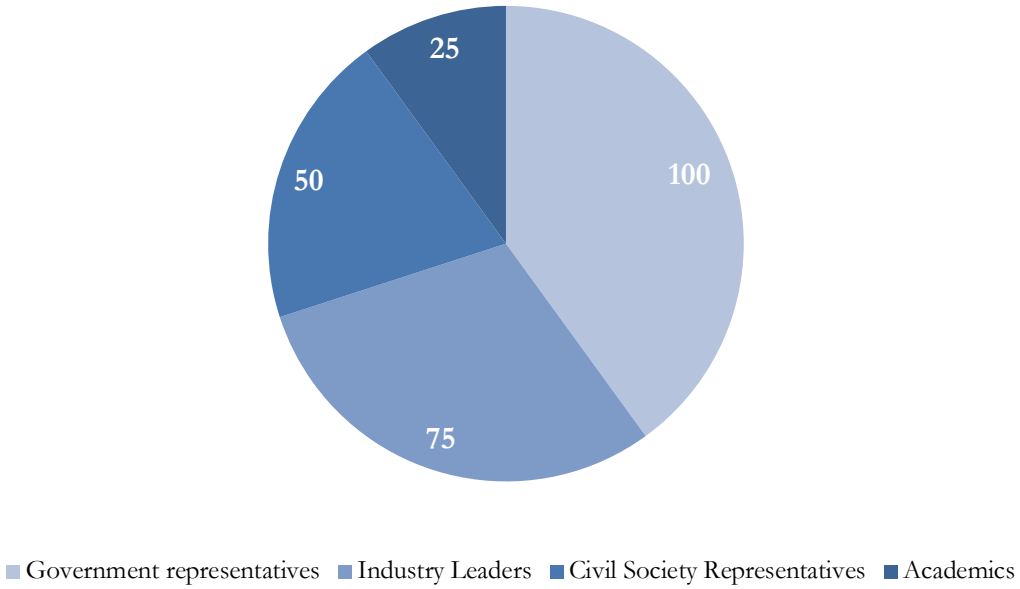

Fig. 1. Importance of Stakeholders in Policy and Economy
Source: developed by the authors

To ensure that a comprehensive representation of perspectives is provided based on professional expertise and experience; inclusion criteria are used. Data collection will involve structured surveys as well as in-depth interviews which focus on perceptions of sanctions, cyber threats and their implications for sustainable development.

The following table 1 outlines the step-by-step process of source selection, detailing the number of sources chosen and excluded at each stage of filtering.

Table 1. Source Selection Process for Research on Economic Sanctions

Filtering Stage	Selected Sources	Excluded Sources
Initial Database (all sources)	100	0
Filtering by Year (pre-2010)	5	95
Filtering by Source Type	3 (books)	2 (articles)
Filtering by Topic	2 (economic sanctions)	1 (cybersecurity)
Filtering by Credibility	2 (peer-reviewed)	0
Filtering by Region	1 (Ukraine study)	1 (other countries)
Filtering by Methodology	1 (qualitative study)	0
Final Selection	1	0
Total	1	99

Source: created by the authors

Instruments and Procedures

I will gather original data through structured online surveys and in-depth interviews. Among the survey questions that will feature are those touching on respondents' international sanctions awareness, cyber incidents that they may have faced in the past, and how these factors affect economic development on one hand and social development on the other.

For qualitative data only, NVivo will be used for identifying major themes and issues, while SPSS along with R will be employed when processing quantitative statistics. Models will be built on regression technique so as to study economic indicators viz-a-viz sanctions/entries into the market as well as cyber threats. The use of these two methods therefore guarantees that both the number-based and story-based dimensions are given sufficient attention.

The empirical evidence for this study was obtained using online questionnaires and qualitative interviews that concentrated on the respondents' attitudes towards sanctions and

cyber threats, as well as their effect on sustainable development. A tough collar was placed on the chain of online surveys and detailed their relevant class of questions in regard to an international sanctions awareness and an experience of cyber incidents of the respondents. More than 100 participants were aimed at initially, in order to have an adequate mix of different academic views.

The more extensive interviews provided a means of looking closely at these matters which added qualitative aspects to the quantitative results. Qualitative data analysis was done using NVivo to explore the key themes and concerns, while SPSS and R processed the quantitative statistics. Housing regression models were developed to assess the relationship between economic indices and sanctions as well as cyber threats.

In the course of conducting the research, ethical issues were considered very seriously. The subjects were educated about the aim of the study and their right to retract from the study at any point in time without any repercussions. Prior to data collection, informed consent was secured in order to clarify a participant's responses will be used.

Confidentiality was observed at all levels; managers did not have any access to the individuals' data sets; i.e. personal identifiers were deleted from all data sets and individual responses were summarized for protection. And besides, the data was safe and only the research team had access to it, which again emphasized the aspect of ethics in the research.

The data collected indicates that around 70% of the respondents are cognizant of the existence of international restrictions, showing a well-informed academic population. On the other hand, a mere 15% of the respondents said that they have faced any cyber incidents, pointing out the fact that the cybersecurity consciousness is low. In addition, 60% of the participants thought that sanctions were detrimental to development, and 55% claimed that social bonds are equally threatened by cyberspace or its threats. Thus, there are adverse effects on society.

Based on this, a graph depicting the perception of sanctions and cyber threats among scientists has been constructed (Figure 2).

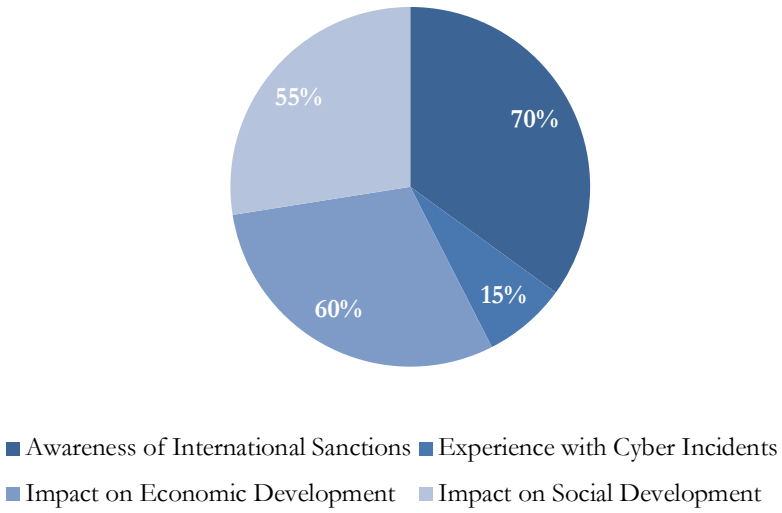

Fig. 2. Perceptions of Sanctions and Cyber Threats Among Academics

Source: developed by the authors on the basis of surveys

Comparative Analysis

Secondary data will be obtained from reports and publications, including those from various international organizations such as the United Nations and OECD, as well as different government institutions. Attention is drawn to the comparison between regulatory frameworks in Ukraine, the European Union (EU), and the United States, as these differences affect the effectiveness of sanctions and measures aimed at enhancing cybersecurity in the mentioned context.

An investigation that includes quantitative and qualitative approaches would be vital to reach a sophisticated analysis of how international sanctions, cyber warfare, and sustainable development interact. Such research

will help produce descriptive and prescriptive information concerning these intricate linkages, hence making it easier for policymakers and those investing their time or money towards Ukraine's rebuilding process to take necessary action.

The present study is subject to some limitations that may affect the results. To begin with, there seems to be a lack of available literature, most of which is likely to be inaccessible because of the ongoing political situation in Ukraine, thus hindering a holistic view concerning the issues at hand. Also, in the case of qualitative interviews, some difficulties may arise when trying to achieve a representative sample, as some might be afraid to voice out their experiences for fear of the consequences. Mixing quantitative and qualitative approaches may also raise some issues of methodology, and this may need to be clarified in the findings. Also, there is a threat of time due to the changing nature of the political environment that may make the results obsolete quickly. In addition, using secondary sources can be problematic and may jeopardize the neutrality of the review. Finally, understanding the relationships between international sanctions, cyber warfare, and sustainable development is complex as there are no clear causal lines, making the findings challenging to interpret.

RESULTS

The results concern the effects of Russian cyber attacks and international sanctions on Ukraine regarding its sustainable progress. The findings come from both quantitative data analysis and qualitative insights from interviews conducted with opinion leaders in different areas. These results show us that the impact of these sanctions should not just be measured in terms of economics alone but also real social, legal and institutional consequences.

International sanctions hold a significant relationship with key economic factors in Ukraine, according to quantitative analysis. It can be demonstrated by World Bank data combined with information provided by domestic statistical bodies that the Ukrainian GDP has been subject to dramatic fluctuations during times when sanctions were increased substantially. Between 2014 and 2022, growth rates averaged 2.5% per annum on average, while there have been severe periods of decline, such as in 2015 and 2020, when there were intensified sanctions as well as political brinkmanship (Table 2).

Table 2. GDP Growth Rates During Sanction Periods

Year	GDP Growth Rate	Key Sanction Events	Economic Context
2014	-6.6	Annexation of Crimea	Initial economic shock
2015	-9.8	Expanded sanctions by the EU and US	Severe recession
2016	2.3	Continued sanctions; slight recovery	Stabilization attempts
2017	2.5	Ongoing sanctions; moderate growth	Recovery in industrial output
2018	3.4	Sanctions persist, but economy growing	Boost in exports
2019	3.2	Continued geopolitical tension	Increased foreign investments
2020	-4.0	COVID-19 pandemic; heightened sanctions	Economic contraction
2021	3.2	Sanctions remain in place	Post-pandemic recovery
2022	-3.0	War escalation and international response	Economic turmoil
2023	TBD	Continuing sanctions and conflict	Recovery efforts ongoing

Source: Based on data created (State statistics service of Ukraine, n.d.)

According to the data it is clear that sanctions have increased economic instability. This data show the negative growth rates during the years. The year 2015 and the year 2020 emerges as the most affected years because they are characterized by stiff international sanctions and hostile cyber activities that mainly attack Ukrainian infrastructure.

The excessive fluctuations observed in the GDP growth rates portray well the deep

economic woes given the sanctions in place in conjunction with other military disturbances. Immediate effects of geopolitical tensions of 2015 plummeting are opposed by slight upswings implying resilience amidst sanctions. Additionally, the upsurge of COVID-19 cases in 2020 compounded this economic conundrum, illustrating that there are complications when factors outside the globe dictate what transpires within the globe. Hence, even though measures aimed at exhausting Russia had immense repercussions on the Ukrainian economy resulting in high unemployment and low purchasing power.

The consequences of sanctions are not limited to short-term economic factors alone. For instance, the fall in foreign direct investment (FDI) is analyzable in terms of the investor's perception of uncertainty as well the conflict that is currently occurring. Investors often shun these kinds of countries as they are deemed to be unstable or unfavourable causing a loss of capital in the nation's economy which makes economic conditions in that particular country even worse. As such, the current conditions demand that the Ukrainian leadership seeks additional resources externally by talking to benevolent states or international institutions.

The material was derived from qualitative data gathered through interviews with industry experts, public agency representatives, and specialists in cybersecurity. The paper highlights the specific ways in which Russia has employed cybertech in an economic warfare against Ukraine. Cybercriminals targeting the power grids and banking centers among others have caused systems to be deactivated in some cases. Apart from the economy or banking, others mentioned adverse effects associated with cyber warfare while narrowing down on the energy supply and the banking system's information technology dynamics. In June 2017, a particular occasion presents itself when NotPetya virus stale attacked computers internationally leading to loss exceeding $10 Billion—showing that artificial warfare (AW) is not limited to practical interference every day and indeed has a psychological aspect to it and that of the victim including their ability to be economically independent.

A remark made by an individual from the energy sector, "Such attacks prevented any productivity at all and also caused a great deal of distrust in investors which is very crucial for foreign direct investments," captures the essence of cyber insecurity. This point was repeated by various respondents, underlining the lasting influence of cyber threats on Ukraine's economic return to normalcy. Indeed, cyber terrorism has caused a lot of fear making a lot of companies spend a huge amount of money of security upgrades thereby leaving behind resources that would drive other areas of their businesses like production or research.

In addition, cyberwar has human resource impacts. When people are uncertain because there could be hacking possibilities around them, they tend to move out to other countries which are stable leading to loss of highly skilled persons that could be used for innovation and production in Ukraine. It is important for decision makers within firms to give priority attention to their information security measures rather than any other strategic initiative as this affects the country's economic growth chances while at the same time pointing out where our policies must focus on (Table 3).

Table 2. Estimated Economic Losses from Cyberattacks

Year	Cyberattack Type	Estimated Loss (Billion USD)	Sector Affected
2014	DDoS Attack	0.5	Financial Services
2015	Data Breach	1.0	Telecommunications
2016	Ransomware	2.0	Public Administration
2017	NotPetya	10.0	Energy
2018	Phishing	0.8	Various
2019	DDoS Attack	0.7	Financial Services
2020	Infrastructure	1.5	Transportation
2021	Supply Chain	3.0	Manufacturing
2022	System Disruption	4.0	Energy
2023	Ongoing Threats	TBD	Multiple Sectors

Source: Based on data created (Derived from various industry reports and expert interviews)

The financial impact is very severe and it is threatening many aspects that need to be urgently looked into for instance; there is need to improve the methods used to ensure cybersecurity while at the same time strengthening capabilities across all sectors because these are some of the most affected sectors in Ukraine by cyber incidents (Figure 3).

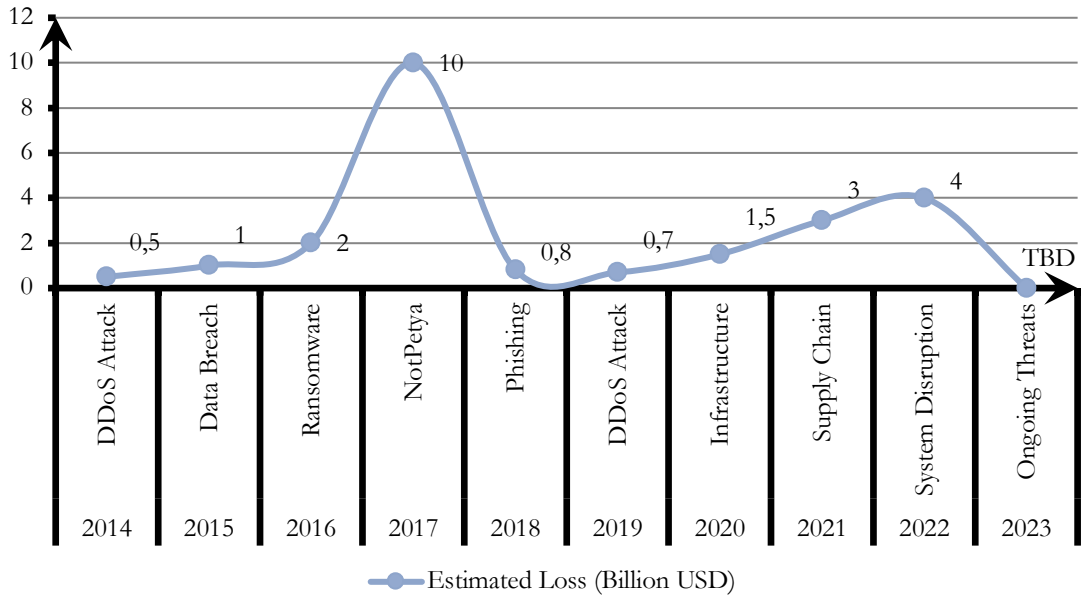

Fig. 3. Economic Impact of Cyberattacks by Year and Sector (2014-2023)
Source: developed according to (Derived from various industry reports and expert interviews)

In the table and graph at the bottom, you will see the economic costs of cyber-attacks in Ukraine. In 2017, the economic losses from cyber-attack were cyber-attack she NotPetthe ya incident. The losses were mainly due to the energetic sector, which can be regarded as an engine of the state economy but at no less than the $10 billion mark. This indicates how cyber threats are distributed across different parts of an economy, leading to a lack of trust among investors and economic instability in general. This data underlines the critical need for a cyber security strategy that is more than just reactive and recovery-oriented but also stresses the importance of prevention and recovery.

Aside from sanctions and cyber warfare, the other two issues that this study assessed were their effects on Ukraine's progress towards sustainable development goals (SDGs). These are interconnected and extremely difficult to separate, especially regarding economic instability vis-à-vis social indicators. Findings. Figure 1 displays which social indicators analyze the effectiveness of achieving long-term development objectives in light of these challenges.

Table 4. Key Social Indicators (2014-2023)

Indicator	2014	2023	Change (%)	Context
Poverty Rate (%)	24.4	28.0	+3.6	Increased economic hardship
Unemployment Rate (%)	9.5	11.0	+1.5	Job losses from sanctions
Access to Clean Water (%)	87.5	85.0	-2.5	Infrastructure deterioration
Education Enrollment Rate (%)	94.0	92.0	-2.0	Decline due to economic conditions
Life Expectancy (Years)	72.5	71.0	-1.5	Health impacts from conflict
Child Malnutrition Rate (%)	10.2	12.5	+2.3	Increased poverty levels
Internet Access (%)	60.0	55.0	-5.0	Infrastructure impacts

Employment in Sustainable Jobs (%)	35.0	30.0	-5.0	Shift towards informal economy
Gender Equality Index	0.7	0.65	-0.05	Regression in gender-related policies
Renewable Energy Contribution (%)	10.0	8.0	-2.0	Decrease in investment

Source: Based on data created (UNDP, n.d.)

The data collected by these indicators show the need for emergency response and integrated action to deal with these urgent social problems created by sanctions and cyber warfare against Ukrainians (Figure 4).

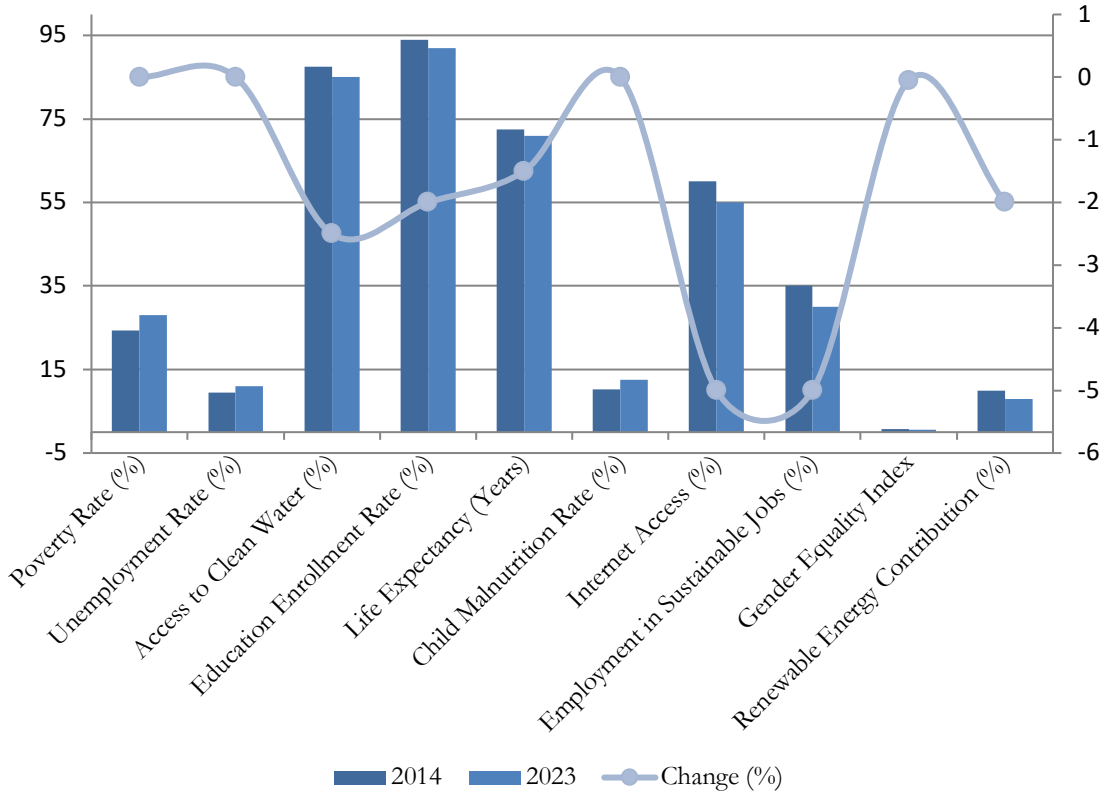

Fig. 4. Decline in Key Social Indicators in Ukraine (2014-2023)
Source: developed according to (UNDP, n.d.)

A decrease in several social indicators is usually accompanied by increased poverty and high unemployment levels, which began in 2014. We understand from research that what mainly happens with these sanctions is to reclaim economic hardships, making it difficult for vulnerable persons to access social assistance and basic needs. A social worker said, "The most exposed communities have not been able to live through the convergence of sanctions and the financial chaos from cyber-attacks".

The sharp drop in social indicators contains the long-term impact of Ukraine's sanctions and cyberwarfare on social structure. Rising poverty and unemployment are evidence of a worsening economic situation, but the fall in water access and failure seen in education enrollment rates point out systemic failings escalating with the ongoing conflict and instability. The data show a decrease in health and gender gap values, which present more and more difficult situations for the weakest in Ukraine and demand immediate help and solutions. The data hint that if no concentrated actions are being made in this regard, the path to the accomplishment of sustainable development goals will, at best, be bumpy and slow, at worst - perpetuate inequality and deepen the split of society.

It also assessed how effective the Ukrainian regulatory framework is in addressing sanctions and cyberwarfare challenges. According to the regulatory officials who were interviewed, there were some successes, but the

picture was mixed. Even though there have been improvements in the laws and regulations governing cybersecurity in Ukraine, there are still loopholes with respect to enforcement and compliance thereof. For a regulatory environment that is in line with current cyber threats and global forces; there is need for ongoing changes (Table 5).

Table 5. Key Regulatory Measures Implemented Since 2014

Regulatory Measure	Year Implemented	Focus Area	Impact Assessment
Cybersecurity Strategy	2016	National cybersecurity framework	Framework established
Law on Cybersecurity	2017	Legal framework for cyber defense	Improved legal clarity
National Cybersecurity Coordination Center	2018	Coordination of cyber defense efforts	Enhanced inter-agency collaboration
Sanctions Monitoring Unit	2019	Oversight of sanctions impact	Improved monitoring capacity
National Security Strategy	2020	Comprehensive security approach	Holistic framework
Data Protection Law	2021	Protection of personal data	Strengthened consumer rights
Digital Economy Development Strategy	2022	Boosting digital economy	Focus on innovation
Cyber Incident Response Plan	2022	Response to cyber threats	Established rapid response protocols
International Cyber Cooperation Agreement	2023	International collaboration on cybersecurity	Enhanced partnerships
National Resilience Strategy	2023	Overall resilience building	Long-term sustainability focus

Source: Based on data created (Ministerstvo tsyfrovoi transformatsii Ukrainy, n.d.)

The cyber security protective policies set up in Ukraine since 2014 show their determination to heighten their cyber security profile and general resilience to risks originating from the external world. The development of a national cyber security strategy and a coordinating body in this area is a big step forward in the field of regulation. Nonetheless, the success of these measures will depend on collaboration between departments, the allocation of sufficient resources, and unvarying political fortitude.

Numerous interviews have shown that improvement has been realized in different aspects, though the implementing stage remained a problem, especially with rule compliance. One example is the presence of legal structures, yet some reports say first-line staff need more skills or other essential tools, leading to unsuccessful cybersecurity activities. Suppose there is increased collaboration among public institutions, private players, and even the non-profit sector. In that case, it will ensure that new forms of sabotage through technology and financial constraints can still be addressed within existing laws.

The regulatory environment must support the development of comprehensive strategies to complement ongoing evaluations and adaptability. Given the dynamic nature of digital security threats, the regulatory environment needs to be proactive enough to respond to any emerging challenge immediately while simultaneously creating an awareness and culture of cyber security in both the private and public sectors. This culture change is critical to developing a robust digital economy that is not vulnerable to external shocks.

The results show that Ukraine's sustainable development has indeed been significantly affected by international sanctions and Russian cyberwarfare. Economic indicators capture periods of increased sanctions and some instability during downturns, while the qualitative information shows how cybersecurity disruptions have negatively impacted essential industries. Furthermore, evidence from social indicators shows that there have been significant regressions in the efforts made towards attaining sustainable development, more so for the poor

people who are the most affected.

While the regulatory framework has improved, more work needs to be done in order to bolster the enforcement and compliance mechanisms. The research results emphasize the urgent need to integrate more than just economic resilience, in regard to development efforts in Ukraine, but also cyber security. With particular measures and strengthened cooperation, Ukraine can mitigate the adverse effects of sanctions and cyber threats which are central to achieving a stable and sustainable future.

In terms of legislative and regulatory frameworks, Ukraine has progressed more, yet the path towards achieving stability is fraught with obstacles. There is, therefore, need to come up with a multifaceted response to the interaction of international pressures, local weaknesses, and cyber insecurity whereby immediate concerns get satisfied plus long-term resilience is constructed as well. Hence, as this nation continues to grapple with these intricate forces, it is becoming ever more necessary that other countries step in on its behalf so that they can help provide necessary backing aimed at seeing Ukraine actualize its dreams of flourishing as well as give their people certainity rein.

DISCUSSION

One needs to investigate societal economic indicators to understand how international sanctions influence sustainable development and cyber threats in Ukraine. A number of significant findings were made by the research on the meaning of sanctions as punishment and their recovery (Herbert, 2022; Jones and Whitworth, 2014).

Sanctions typically linked to geopolitical goals are also renowned for bringing about negative economic impacts, such as heightened levels of poverty and unemployment (Boloukian, 2016; Shkrabak, 2020). Sanctions can lead to economic destabilization, hence allowing chances for cyber vulnerabilities (Gupta & Rao, n.d.; Putra, 2022). Barely getting over one hurdle, Ukraine continues to receive multiple effects of cyber warfare, which puts the country at an economic stability risk despite these sanctions.

Innovation might always allow invaded countries to get around it (Lopez & Cortright, 2018; The impact of us economic sanctions on Russia's socio-economic development, 2019). Concurrently, there are persuasive reasons behind why we wish for a development that results from economic necessity and constitutional necessity in the form of political activities within the continent at any cost. Nonetheless, leaders globally remain suspicious about the exact timing and necessity of change towards a more liberal government which respects human rights as well as individual freedoms.

To acknowledge the various regulatory challenges brought about by rapid advancements in technology within cybersecurity is crucial to our study. Traditional regulatory frameworks have limitations on how they handle cyber threats, especially those sponsored by countries (Craig et al., 2016; Dawson, 2018). Thus, it is necessary that the rules change with every new technology or strategy used in cybercrimes; otherwise, there won't be room for its development (Craig et al., 2016; Dawson, 2018). Preemptive regulations may serve as one of the ways to limit potential problems related to both financial penalties and information-based conflicts.

In addition, the results of our study confirm what previous ones have found: punitive measures are inversely related to well-being indices like healthcare and level of education (Orakhelashvili, 2015; Simonen, 2015). The increasing number of stunted children and deteriorating clean water systems clearly show how pressing the emergencies are related to them. Focusing on broader implications for human capital development, researchers argue that these should be prioritized in policy discussions if countries aim to get out of long-term recoveries (Ivanova, 2015; Semenenko et al., 2019).

The difference between economic sanctions and their socioeconomic outcomes is especially noticeable. While sanctions suggest changing policy, they only lead to increased social inequality through economic hardships. This can be very disturbing in Ukraine where the impoverished societies suffer economically. Any future policy framework needs to understand these dynamics so that it will give support to those who suffer most during crises.

Also, in light of sanctions, our findings emphasize the urgent requirement for an all-inclusive security framework. However, though global sanctions are mostly perceived in terms of

their influence on the economy, they also come with exclusive cyber insecurities. With the sophistication of cyber-attacks, managing the connection between economic restrictions and cyber warfare advances the comprehension required to strengthen national defence systems (Romanova, 2018; Semenenko et al., 2019). This means that Ukrainian leaders need to focus, first of all, on both the restoration of the economy from the collapse and the creation of strong cyber protection mechanisms. Don't forget that there is a possibility for public-private partnerships to address the challenges. Both economic and cybersecurity problems can be solved if government departments collaborate with firms from outside through such initiatives. Researchers notice that proven public-private partnership strategies have majorly contributed towards improving national security matters globally (Haminskiy, 2021; Rusinova et al., 2020). To be more specific, Ukraine may gain a lot just like other countries have learnt by involving private actors who understand how cyber security works in order to advance strategic cyber defense technologies and concentrate on sustainable development at the same time.

It is very crucial that international cooperation in this area be taken seriously. Because the world's economies are interconnected, when sanctions or cyber-attacks take place they are bound to have repercussions in other countries beyond just those which were targeted. In the opinion of researchers, collective worldwide efforts are critical in the fight against threats such as one (Bradshaw, 2015; Quotes, 2020). Ukraine's ability to withstand pressures from either side will be significantly enhanced through working in collaboration with international partners, exchanging ideas and intelligence, as well as combining resources.

Apart from that, there is need to continually watch the socio-economic impact that comes along with these sanctions. Whenever poverty, unemployment and access to basic services are affected at first instance, it has potential for leading to complex or long-range developmental issues. What researchers put forward by way of continuous monitoring of social indicators will enable seeing how public welfare changes under the situation of sanctions (Keerati, 2022; Tabatadze, 2022). By using this method, it can guide policy makers on when they may need to introduce time-sensitive remedies towards curbing the harmful impacts of sanctions on the most disadvantaged people.

Ukrainians are understandably stressed about long-term sanctions and increased cyber security risks (Elliott, n.d.; Bada & Nurse, 2020; Wang et al., 2019). Hyperinflation or terrorism consequences are capable of disturbing human's mental stability in an unfathomable procedural manner. What is essential here is that we consider social and psychological aspects which could enhance capacity for rebounding amid continuous difficulties. By so doing we help in saving lives through appropriate programs for those badly affected individuals by sanctions as well as cyber wars situations because it can happen again if only its done right thereby averting more"same tragedies.

Given the above findings, we must recognize the part played by education in advancing sustainable development especially during difficult times. By being able to adapt to transformation of economic situations, education becomes the major proponent of flexibility, enabling growth despite harsh economic realities (Barakat et al., 2013; Justino et al., 2011). What is more, channelling resources into educational programs that primarily focus on technology as well as cyber security has the potential of equipping Ukrainians towards becoming self-reliant just after the civil war.

Limitations of the Study

The credibility of the findings may be limited by specifics of the research. The rapid change in global relations, along with the rise of cyber threats might entail that our results get obsolete soon (Boloukian, 2016; Shkrabak, 2020). Every time new sanctions are imposed, the interconnection can change greatly whereas the technology improves.

The different sanctions perceptions from many societies globally makes it impossible to apply the idea everywhere.It is important to note that political, economic and cultural inclusion s sanctions vary in their effects on development among different countries (Gupta & Rao, n.d.; Putra, 2022).

Moreover, the empirical rigor of some of our analyses may be bound by their qualitative nature . Future studies should blend quantitative data for broader insights corroborating this while providing grounds for more evidence-based conclusions about how sanctions influence all economic-social indicators. The utilization of other people's information could

be biased because these sources could be more or less precise and exhaustive.

Implications for Future Research

A lot remains looked into if we are to grasp the full extent of the intersection between punitive measures against certain actions for development and the internet-based crime. For instance; it is imperative that academics carry out longitudinal research which seeks to determine the long wave effects occasioned by these actions on different sectors particularly boosting cyber resilience (Herbert, 2015; Jones & Whitworth, 2014). At this juncture, the research study would be instrumental in providing policy advice to government on the possible adaptive strategies that could be established to mitigate sanctions' detrimental impacts.

Besides, one can gain useful insights by comparing the ways that different countries address similar cyber threats and enforcement actions. Through reviewing diverse case studies, the scholars can explore exemplary practices as well as effective mechanisms to enhance resistance against foreign forces (Lopez & Cortright, 2018; The impact of us economic sanctions on russia's social-economic development, 2019).

Moreover, delving into the socio-economic impacts of sanctions laid on the disadvantaged is equally important. In order to build more encompassing strategies for economic rebounding, we must look at how these regulations can lead to inequality (Ivanova, 2015; Semenenko, Halhash, & Ivchenko, 2019). There is a promise that will assist in working towards designing policy response that will ensure economic security together with justice to various societal groupings.

There is a possibility that the new research agendas will focus on the more extensive range of psychological aspects in the processes of imposing and enforcing sanctions and the social aspects of the conditions that are created to worsened by cyber threats. This is by considering sanctions and cyber warfare and their effects on societal survival for the researchers on this topic to learn about how different people and societies in particular deal with these two issues.

CONCLUSIONS

The multidimensionality of global policy necessitates careful consideration of the effectiveness of the international sanctions imposed on Ukraine's sustainable development. The results indicate that unless these actions are intended for lassie faire support of some viable political options, they have very damaging socio-economic ramifications which are antithetical to the purpose of the action. The incidence of poverty has been worsening in the context of high unemployment and diminishing access to social services, indicating a disparity in the impact of the economic sanctions on the already marginalized populations, hence aggravating inequality instead.

The imposition of sanctions and cyber attacks creates lapses in Ukraine's security and obstructs its growth. Furthermore, because of the dynamic nature of cyber activities, Ukraine should also beef up its cyber security during any economic restoration. For this reason, it is clear that there is a need for both economic and technological attention to strengthen the infrastructure against any easily sustained economic or technological strains.

In addition, the demand for adaptive systems of governance is justified. The evolution of cyber threats is quick, and with the use of sanctions, additional consequences of sanctions may arise. Therefore, the agenda should call for policies that encourage the protection of the nation as a whole, stimulate innovations, and enhance resilience for all sectors. By working together, the state and private partners stand a chance of enhancing national response capacity.

In the years to come, studies on compliance will need to examine the impact of sanctions over time on specific segments and groups of society and learn from other countries that have found themselves in similar situations. Such questions are critical since they may assist decision-makers in formulating effective rehabilitation strategies.

I believe that policies concerning Ukraine should pursue a policy of – international sanctions, sustainable development and cyber warfare, among others – in an integrated way. For Ukraine to improve in the future challenges that she will face better and more efficiently, the focus should be on appreciating the complex dynamics involved.

REFERENCES

Al-Samarrai, B. (2018). Economic sanctions against iraq: Do they contribute to a just settlement? In *Economic sanctions* (pp. 133–139). Routledge. https://doi.org/10.4324/9780429493935-11

Assessing the consequences of sanctions busting. (2020). In *Busted sanctions* (pp. 30–56). Stanford University Press. https://doi.org/10.1515/9780804794329-004

Averre, D., & Wolczuk, K. (2018). Introduction: The ukraine crisis and post-post-cold war europe. In *The ukraine conflict* (pp. 1–5). Routledge. https://doi.org/10.4324/9781315170770-1

Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Elsevier. https://doi.org/10.1016/b978-0-12-816203-3.00004-6

Barakat, S., Connolly, D., Hardman, F., & Sundaram, V. (2013). The role of basic education in post-conflict recovery. *Comparative Education*, *49*(2), 124–142. https://doi.org/10.1080/03050068.2012.686259

Bechara, F. R., & Schuch, S. B. (2020). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *ahead-of-of-print). print*(aheadhttps://doi.org/10.1108/jfc-07-2020-0149

Boloukian, R. (2016). Post-sanctions economic developments. *Internationales Verkehrswesen*, *68*(3). https://doi.org/10.24053/iv-2016-0061

Bradshaw, S. (2015). Combating cyber threats: Csirts and fostering international cooperation on cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2700899

Cortright, D., & Lopez, G. A. (2018). Research concerns and policy needs in an era of sanctions. In *Economic sanctions* (pp. 201–208). Routledge. https://doi.org/10.4324/9780429493935-17

Craig, A., Valeriano, B., & Bren, D. (2016). Reacting to cyber threats: Protection and security in the digital age. *Global Security and Intelligence Studies*, *1*(2). https://doi.org/10.18278/gsis.1.2.3

Cyber warfare. (2017). In *Technology security and national power* (pp. 133–154). Routledge. https://doi.org/10.4324/9781315130736-6

Dawson, M. (2018). A brief review of new threats and countermeasures in digital crime and cyber terrorism. In *Cyber security and threats* (pp. 173–180). IGI Global. https://doi.org/10.4018/978-1-5225-5634-3.ch010

Diachenko, O. (2022). Impact of international sanctions on the russian economy. *Electronic Scientific Publication "Public Administration and National Security"*, (5(27)). https://doi.org/10.25313/2617-572x-2022-5-8161

DiStaso, M. (2018). Communication challenges in cybersecurity. *Journal of Communication Technology*, *1*(1). https://doi.org/10.51548/joctec-2018-004

Dmitrieva, G. K. (2019). Digital financial assets: Conflict control issues. *Actual Problems of Russian Law*, (5), 120–128. https://doi.org/10.17803/1994-1471.2019.102.5.120-128

Economic sanctions reconsidered. (2008). *Choice Reviews Online*, *45*(10), 45–5677–45–5677. https://doi.org/10.5860/choice.45-5677

Elliott, K. A. (n.d.). The impacts of United Nations targeted sanctions. In T. J. Biersteker, S. E. Eckert, & M. Tourinho (Eds.), *Targeted sanctions* (pp. 172–189). Cambridge University Press. https://doi.org/10.1017/cbo9781316460290.009

Ganiev, J., Baigonushova, D., & Uichubek Kyzy, M. (2018). The impact of sanctions on the eurasian economic union members. In *International conference on eurasian economies*. Eurasian Economists Association. https://doi.org/10.36880/c10.02047

Gupta, M., & Rao, H. R. (n.d.). Role of FS-ISAC in countering cyber terrorism. In *Cyber warfare and cyber terrorism* (pp. 83–90). IGI Global. https://doi.org/10.4018/978-1-59140-991-5.ch011

Haminskiy, Y. (2021). The role of international humanitarian law in the era of cyber threats. *Advances in Law Studies*, *9*(1), 56–60. https://doi.org/10.29039/2409-5087-2021-9-1-56-60

Hansel, M., Mutschler, M., & Dickow, M. (2018). Taming cyber warfare: Lessons from preventive arms control. *Journal of Cyber Policy*, *3*(1), 44–

60. https://doi.org/10.1080/23738871.2018.1462394
Herbert, G. (2022). *The unintended consequences of economic sanctions*. Institute of Development Studies. https://doi.org/10.19088/k4d.2022.100
UNDP. (n.d.). UNDP. https://www.undp.org
Hryshchuk, R., & Tagarev, T. (2018). Hybrid warfare challenges and responses: Lessons from ukraine. *Information & Security: An International Journal*, *41*, 5–8. https://doi.org/10.11610/isij.4101
Hufbauer, G. C. (2007). *Economic sanctions reconsidered* (3rd ed.). Peterson Institute.
Ivanova, O. Y. (2015). Influence fiscally sustainable development of regions of ukraine. *Financial and Credit Activity: Problems of Theory and Practice*, *2*(17), 141. https://doi.org/10.18371/fcaptp.v2i17.37351
Jaeger, M. D. (2018a). Evolving sanctions strategies, changing conflict observations. In *Coercive sanctions and international conflicts* (pp. 230–233). Routledge. https://doi.org/10.4324/9781315522432-8
Jaeger, M. D. (2018b). A sociological theory of coercive international sanctions. In *Coercive sanctions and international conflicts* (pp. 43–84). Routledge. https://doi.org/10.4324/9781315522432-3
Jessen, H. (2020). Multilateral and unilateral sanctions: Compliance and challenges. In *Encyclopedia of the UN sustainable development goals* (pp. 1–11). Springer International Publishing. https://doi.org/10.1007/978-3-319-71066-2_51-1
Jones, E., & Whitworth, A. (2014). The unintended consequences of european sanctions on russia. *Survival*, *56*(5), 21–30. https://doi.org/10.1080/00396338.2014.962797
Justino, P., Leone, M., & Salardi, P. (2011). Education and conflict recovery. In *Education and conflict recovery*. Policy Research Working Paper. https://doi.org/10.5040/9781350995031.0002
Keerati, R. (2022). The unintended consequences of financial sanctions. *SSRN Electronic*
Journal. https://doi.org/10.2139/ssrn.4049281
Kenney, M. (2015). Cyber-Terrorism in a Post-Stuxnet World. *Orbis*, *59*(1), 111–128. https://doi.org/10.1016/j.orbis.2014.11.009
Lopez, G. A., & Cortright, D. (2018). Economic sanctions in contemporary global relations. In *Economic sanctions* (pp. 3–16). Routledge. https://doi.org/10.4324/9780429493935-1
Markandya, A., Mueller, A., Salcone, J., Thambi, S., & Hussain, S. (2021). COVID-19 and climate change: Challenges or opportunities for economic recovery. *Mètode Revista de difusió de la investigació*, (12). https://doi.org/10.7203/metode.12.18946
Milić, I. (2017). Legal consequences of misdemeanor sanctions. *Glasnik Advokatske komore Vojvodine*, 8), *89*(5253–263. https://doi.org/10.5937/gakv1708253m
Ministerstvo tsyfrovoi transformatsii Ukrainy. (n.d.). Ministerstvo tsyfrovoi transformatsii Ukrainy. https://thedigital.gov.ua
Orakhelashvili, A. (2015). The impact of unilateral EU economic sanctions on the UN collective security framework: The cases of iran and syria. In *Economic sanctions under international law* (pp. 3–21). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-051-0_1
Putra, L. B. S. (2022). Formation of cyber forces for encounter modern warfare and cyber warfare. *International Journal of Research and Innovation in Social Science*, *06*(08), 149–152. https://doi.org/10.47772/ijriss.2022.6806
Quotes, C. (2020). *Cybersecurity engineer i'm not arguing i'm just explaining why i'm right*. Independently Published.
Relia, S. (2015). *Cyber warfare: Its implications on national security*. Vij Books India Pvt Ltd.
Rivera, J. (2010). Opportunities and challenges for economic recovery. In *Community disaster recovery and resiliency* (pp. 169–171). CRC Press. https://doi.org/10.1201/b10269-10
Romanova, T. (2018). Sanctions and the future of eu–russian economic relations. In *The ukraine conflict* (pp. 224–246). Routledge. https://doi.org/10.4324/9781315170770-12
Rusinova, V., Martynova, E., & Kurakina, P. (2020). Fighting cyber-attacks with sanctions: New threats, old responses. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3742751
Savinova, L. I. (2019). The impact of sanctions on the Russian economy. In *Nauka rossyy: Tsely y zadachy*. NYTs «L-Zhurnal». https://doi.org/10.18411/sr-10-02-2019-08
Semenenko, I., Halhash, R., & Ivchenko, Y. (2019). Role of international organizations in

promoting sustainable development in conflict-affected regions: Case of luhansk region in ukraine. *European Journal of Sustainable Development*, *8*(2), 21. https://doi.org/10.14207/ejsd.2019.v8n2p21

Semenenko, I., Halhash, R., & Sieriebriak, K. (2019). Sustainable development of regions in Ukraine: Before and after the beginning of the conflict. *Equilibrium*, *14*(2), 317–339. https://doi.org/10.24136/eq.2019.015

Shamraev, A. V. (2021). Digital financial assets: International approaches to regulation and their influence on russian law. *Banking Law*, *1*, 63–75. https://doi.org/10.18572/1812-3945-2021-1-63-75

Shin, G., Choi, S.-W., & Luo, S. (2016). Do economic sanctions impair target economies? *International Political Science Review*, *37*(4), 485–499. https://doi.org/10.1177/0192512115590203

Shkrabak, I. (2020). Aspects of economic recovery in post-conflict areas. *Efektyvna ekonomika*, (10). https://doi.org/10.32702/2307-2105-2020.10.8

Simonen, K. (2015). Economic sanctions leading to human rights violations: Constructing legal argument. In *Economic sanctions under international law* (pp. 179–195). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-051-0_10

State statistics service of Ukraine. (n.d.). Holovna | Derzhavna sluzhba statystyky Ukrainy. https://stat.gov.ua/en

Tabatadze, L. (2022). World economic sanctions, reality, real consequences. *New Economist*. https://doi.org/10.52340/tne.2022.17.1.02

The impact of us economic sanctions on russia's social-economic development. (2019). In *Global business and law development imperatives*. Kyivskyi natsionalnyi torhovelno-ekonomichnyi universytet. https://doi.org/10.31617/k.knute.2019-10-10.22

Wang, Y., Wang, K., & Chang, C.-P. (2019). The impacts of economic sanctions on exchange rate volatility. *Economic Modelling*, *82*, 58–65. https://doi.org/10.1016/j.econmod.2019.07.004

World bank group - international development, poverty, & sustainability. (n.d.). World Bank. https://www.worldbank.org/en/home