ECONOMIC
SECURITY COUNCIL
of UKRAINE

CYBER WARFARE:
SANCTIONS AND RESPONSIBILITY

Dr. Ilona KHMELEVA, Dr. Bohdan VESELOVSKYI

2024

EXECUTIVE SUMMARY

Cyber aggression is a severe challenge for global security. The development of international regulations and new policy strategies often does not catch up with the emergence of new cyber threats. In addition, cyber instruments are increasingly integrated into the warfare toolkit, through which some states exert illicit influence.

Ukraine's experience in countering Russia's cyber aggression is vital for forming new approaches – both in the political and military dimensions. Although democratic states have developed effective strategies to counter hybrid threats and safeguard their interests, the evolving security landscape necessitates greater proactivity and coordination. Deterrence is insufficient to protect sovereignty and national interests. Increasingly important is the strategy of depriving authoritarian regimes of the tools of cyber aggression, in particular through the introduction of countermeasures. The main challenges are the attribution of cyberattacks not only to hacker groups but also to states, as well as the gradual application of sectoral sanctions and greater control over the supply chains of software and other technologies. A responsible attitude of private companies and comprehensive dialogue between governments and business will play a key role.

Solidarity, as the main principle of modern cyber diplomacy, should aim at two goals: first, joint prosecution of violators for acts of cyber aggression and war crimes. Second, the joint formation of red lines regarding large-scale cyberattacks against critical infrastructure. These acts should be considered a violation of the principle of non-use of force in international law and a basis for individual or collective self-defense.

1. CYBER AGGRESSION AS A THREAT TO GLOBAL SECURITY

1.1. The Russian Federation's aggression is multi-domain in character[1]. Conventional modes of Russian attacks are frequently accompanied or facilitated by cyberattacks. As Russian aggression has demonstrated that cyberattacks often happen in parallel with other unlawful interference, Ukraine's experience shall be used by other countries to improve their resilience.

Severe cyberattacks[2] against banks and government institutions, including the Ministry of Defense, preceded and continued during the 2022 full-scale invasion. Several hours before Russian troops began shelling Ukrainian cities and invading the country, a cyberattack on Ukraine's satellite Internet service[3] had begun.

Cyberattacks have also worsened civilian suffering. For example, in the autumn and winter of 2022-2023, after a series of cyberattacks on the energy sector[4], Russia launched several waves of missile attacks on energy infrastructure[5]. One of the most recent cyberattack examples was on the largest Ukrainian telecom operator, Kyivstar, which led to the destruction of about 40 percent of its supporting infrastructure[6]. Moreover, Russia is attacking not only Ukraine but also its international allies. The EU institutions, as well as national governments and parliaments, are under constant cyberattacks[7]. According to the Joint Cybersecurity Advisory, recently issued by the Bundesamt für Verfassungsschutz (BfV) together with the Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) and other international partners, the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) is running a cyber-group targeting critical infrastructure globally[8]. Thus, intensified Russian cyber warfare poses a threat to global security.

The ESCU's analysis[9] of the Russian cyberattacks demonstrated that there were different types of correlations with conventional strikes. Based on the subject, there are geographical and sectoral correlations. There are preparatory, synchronous, and retaliatory attacks based on the temporal criteria. The Russian war strategy fully integrates hybrid instruments. Moreover, according to the State Service of Special Communications and Information Protection of Ukraine[10], in 2024, the number of Russian hacker attacks increased by 19%. There is a shift in the focus of enemy hackers to everything that is directly related to the theater of war and supply chains.

1.2. Cyberattacks are also used to undermine global stability and democracy. They often amplify the detrimental effects of other hybrid instruments, such as massive disinformation campaigns or acts

[1] https://cip.gov.ua/en/news/doslidzhennya-zv-yazok-mizh-kiberatakami-konvenciinimi-ta-informaciinimi-atakami-v-ukrayini-vidpovidaye-rosiiskii-koncepciyi-gibridnoyi-viini
[2] https://www.theguardian.com/world/2022/feb/16/ukraine-accuses-russia-of-cyber-attack-on-two-banks-and-its-defence-ministry
[3] https://www.reuters.com/business/aerospace-defense/satellite-firm-viasat-probes-suspected-cyberattack-ukraine-elsewhere-2022-02-28/
[4] https://www.bbc.com/news/technology-61085480
[5] https://www.iea.org/commentaries/russias-attacks-on-ukraines-energy-sector-have-escalated-again-as-winter-sets-in
[6] https://en.interfax.com.ua/news/general/955839.html
[7] https://www.politico.eu/article/europe-cyberattacks-russia-china-uk-ministry-of-defence-hacks/
[8] https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2024/2024-09-05-joint-cyber-security-advisory-3.html
[9] https://reb.org.ua/en/reporting/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi-6yvkk2
[10] https://cip.gov.ua/en/news/russian-hackers-adopting-new-tactics-ssscip-report

of sabotage, posing threats to the critical infrastructure and economy. According to recent research by WELT AM SONNTAG and "Politico," Russia is engaging in what is described as a "shadow war," which includes launching severe cyberattacks against European infrastructure[11]. For example, Russian hackers have recently disrupted the operation of at least four Eutelsat satellites from France and one satellite belonging to the Luxembourg company SES[12].

Military and intelligence experts have indicated that Russia employs a full range of tactics: from influencing political discussions and launching cyberattacks on critical infrastructure to large-scale sabotage and assassinations.

Independent researchers demonstrate that the number of state-organized cyberattacks is growing steadily[13]. And while states have traditionally been hesitant to make political attributions of cyberattacks, new security challenges are changing this practice.

For example, in May 2024, the EU made an official statement on continued malicious behavior in cyberspace by the Russian Federation[14], strongly condemning the cyber campaign conducted by the Russia-controlled Advanced Persistent Threat Actor 28 (APT28) against Germany and Czechia. The European countries highlighted Russia's continuous pattern of irresponsible behavior in cyberspace by targeting democratic institutions, government entities, and critical infrastructure providers across the European Union and beyond. Simultaneously, NATO published a similar statement, blaming Russia for intensifying its campaign of activities, which included sabotage, acts of violence, cyber and electronic interference, disinformation campaigns, and other hybrid operations[15].

Another striking example took place in August 2024, when U.S. government officials blamed Iranian hackers for breaking into Donald Trump's presidential campaign[16].

According to the report by the International Monetary Fund[17], global financial stability is also under threat from the increasing frequency and sophistication of cyberattacks. In the past two decades, nearly one-fifth of reported cyber incidents have affected the global financial sector, causing $12 billion in direct losses to financial firms. This tendency creates another challenge: cyberattacks may be used to ruin the adversary states' national economies. For instance, attacks on critical infrastructure may cause economic damage, worsen the investment climate, and paralyze normal activities of state institutions and services.

1.3. Cyber solidarity as a principle of modern diplomacy is transforming security approaches. As hybrid threats are blurring national borders, national sovereignty needs more efficient protection. Coordination of all efforts is the only key to success.

[11] https://www.welt.de/politik/deutschland/plus254516486/Russlands-Kampf-gegen-den-Westen-Wie-Putin-in-Europa-zuendelt.html
[12] https://nos.nl/nieuwsuur/collectie/13903/artikel/2544559-rusland-saboteert-zes-europese-satellieten-ook-nederlandse-tv-geraakt
[13] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[14] https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/
[15] https://www.nato.int/cps/uk/natohq/official_texts_225230.htm
[16] https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-on-iranian-election-influence-efforts
[17] https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/

Microsoft Digital Defense Report 2024[18] stipulates that cyberattacks are on the rise, and the pace of nation-state-sponsored attacks has escalated to the point there is now effectively constant combat in cyberspace. Thus, policy recommendations include more coordinated responses:

- establishing firm countermeasures in response, including targeted sanctions, among other options;
- working more on lawful collective countermeasures;
- clarifying red lines and ensuring that state-sponsored cyber intrusions are not unpunished.

An excellent example of such approaches is the United States International Cyberspace and Digital Policy Strategy[19]. This document focuses on building broad digital solidarity. In a classic understanding, it is a willingness to work together on shared goals, stand together, help partners build capacity, and provide mutual support. However, this strategy also incorporates another element of solidarity – coordinated actions to hold criminal and malign actors accountable.

Ukraine also takes a leading position in the formation of new approaches to security architecture. Countering cyber aggression is included in many recently signed bilateral security agreements. For example, the Agreement on security cooperation between Ukraine and France[20] stipulates that "the Participants will work together to enable Ukraine to detect, deter and disrupt any cyber aggression, cyber espionage, including through greater cyber resilience and critical infrastructure protection from cyberattacks." And Bilateral security agreement between Ukraine and the United States of America[21] formally links conventional and hybrid attacks against Ukraine, stating the need to "improve the cyber resilience of its critical infrastructure, especially energy facilities, against aerial strikes." The document also provides for strengthening cyber defenses against malicious cyber activities by Russia and other hostile state and non-state actors, thus highlighting the global character of this challenge.

Defining cyber defense as one of its core tasks, NATO has also made some significant geopolitical steps[22]:

- At the 2023 NATO Summit in Vilnius, Allies endorsed a new concept to enhance the contribution of cyber defense to NATO's overall deterrence and defense posture and launched NATO's Virtual Cyber Incident Support Capability (VCISC) to support national mitigation efforts in response to significant malicious cyber activities.
- At the 2024 NATO Summit in Washington, D.C., Allies agreed to establish the NATO Integrated Cyber Defense Centre to enhance network protection, situational awareness, and the implementation of cyberspace as an operational domain.

[18] https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
[19] https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/.
[20] https://www.president.gov.ua/en/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-89005
[21] https://www.president.gov.ua/en/news/dvostoronnya-bezpekova-ugoda-mizh-ukrayinoyu-ta-spoluchenimi-91501
[22] https://www.nato.int/cps/en/natohq/topics_78170.htm

2. CYBER SANCTIONS AND OTHER RESTRICTIVE MEASURES

2.1. Cyber sanctions have developed as a new security tool. Autonomous cyber regimes provide for the sustainability of sanctions and enable the emergence of unique approaches.

The European Union has developed a clear and unified approach to counter malicious cyber activities that threaten its security. In June 2017, the EU created the Cyber Diplomacy Toolbox, which marked a critical step towards a common EU response to cyber threats. This initiative enables the EU and its member states to use a range of Common Foreign and Security Policy (CFSP) tools, including sanctions, to prevent and respond to harmful cyber actions against the EU and its members. To put the Toolbox into action, the EU adopted two legal measures in May 2019 – Council Regulation (EU) 2019/796 and Council Decision (CFSP) 2019/797 – providing the basis for sanctions on individuals and organizations responsible for significant cyberattacks that threaten the EU's security.

Sanctions under this framework can apply to those who plan, support or encourage significant cyber incidents, especially those that disrupt critical infrastructure or economic stability. Measures can include freezing assets and imposing travel bans on those involved. The sanctions are imposed by unanimous decision from the Council, following a proposal by any member state or the High Representative, and the EU maintains an updated list of sanctioned individuals and entities. In May 2022, the Council extended this framework until 2025[23], underscoring the EU's commitment to cyber resilience. In June 2024, the EU sanctioned six individuals linked to cyberattacks, including those deploying malware like "Conti" and "Trickbot." The EU's approach generally targets non-state actors to avoid directly attributing attacks to state actors, respecting member states' sovereignty[24].

The United States also has a cyber sanctions regime, established through Executive Orders 13694 (2015) and 13757 (2016)[25], which targets individuals and groups responsible for cyber activities threatening national security or economic stability. The U.S. sanctions can apply to those involved in hacking, ransomware attacks, or intellectual property theft. Sanctioned individuals may face asset freezes, financial restrictions, and travel bans, effectively cutting off their access to the U.S. financial system. Notable sanctions have targeted groups like North Korea's Lazarus Group and Russia's GRU for ransomware attacks like NotPetya and WannaCry. The U.S. often coordinates these sanctions with international allies, amplifying the deterrent effect, and is considering sectoral restrictions, such as blocking access to critical technology, especially for state-linked cyber actors.

These sanctions have disrupted the financial networks supporting cybercriminal activities, reducing the resources available to threat actors and hindering their ability to conduct large-scale cyber operations. The U.S. cyber sanctions are often coordinated with international allies, including the European Union and the United Kingdom[26]. Recent trends indicate a potential shift from personal sanctions to broader, sectoral restrictions, such as limiting access to technology critical for cyber

[23] https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/
[24] https://www.consilium.europa.eu/en/press/press-releases/2024/06/24/cyber-attacks-six-persons-added-to-eu-sanctions-list-for-malicious-cyber-activitiescyberattacks-against-eu-member-states-and-ukraine/
[25] https://www.state.gov/cyber-sanctions/
[26] https://www.state.gov/taking-joint-action-against-cybercriminals/

capabilities, particularly for state-linked actors involved in espionage or attacks on U.S. infrastructure.

In response to escalating cyber threats, the United Kingdom implemented the Cyber Sanctions (EU Exit) Regulations 2020[27], establishing a robust framework to deter and respond to malicious cyber activities that compromise national security, economic stability, and the effective functioning of international organizations. This post-Brexit legislation aligns with global efforts, mirroring the approaches of the European Union and the United States while addressing the UK's specific security concerns. The regulations empower the Secretary of State to designate individuals or entities involved in relevant cyber activities, imposing sanctions including asset freezes, travel bans, and prohibiting making funds available.

The Office of Financial Sanctions Implementation (OFSI) within HM Treasury is responsible for enforcing financial sanctions, providing guidance[28] to ensure compliance and maintain the list of designated persons. The UK's cyber sanctions framework complements international efforts, aligning with the EU's Cyber Diplomacy Toolbox and the U.S. cyber sanctions regime.

In December 2021, Australia introduced its own autonomous cyber sanctions regime, allowing targeted sanctions on individuals or groups responsible for major cyber incidents. Under this framework, the Minister for Foreign Affairs can impose financial restrictions and travel bans on those who engage in or support significant cyber incidents affecting Australia or other countries. Australia's regime is broad, applying to cyber threats from any location worldwide. For example, in October 2024, Australia imposed sanctions on three Russian cybercrime group Evil Corp leaders, known for ransomware attacks causing severe financial damage.

A "cyber incident" is defined as a cyber-enabled event that results in or seeks to cause harm to Australia or another country. The application of the regime is reserved for the most egregious situations of international concern. The relevant legislation includes the Autonomous Sanctions Act 2011 and the Autonomous Sanctions Regulations 2011. Unlike country-specific sanctions, this thematic regime applies to sanctionable conduct worldwide. The regime imposes targeted financial sanctions, including asset freezes and travel bans on designated individuals and entities. Before making a designation or declaration under the regime, the Minister for Foreign Affairs must obtain written agreement from the Attorney-General and consult with other appropriate ministers. The Department of Foreign Affairs and Trade (DFAT) oversees the implementation and enforcement of these sanctions. Entities and individuals are required to comply with the sanctions, and violations can result in significant penalties[29].

In summary, these countries have created frameworks to impose sanctions on individuals and entities engaged in harmful cyber activities to disrupt and deter cyber threats. By coordinating internationally, the EU, U.S., UK, and Australia strengthen their cyber defenses, protecting infrastructure and economies from increasingly sophisticated digital attacks.

[27] https://www.legislation.gov.uk/uksi/2020/597/made
[28] https://www.gov.uk/government/publications/cyber-sanctions-guidance/cyber-sanctions-guidance
[29] https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/significant-cyber-incidents-sanctions-regime

Such comparative overview of the abovementioned national regimes may be provided:

Aspect	U.S.	EU	UK	Australia
Legal Framework	Executive Orders 13694 & 13757	Cyber Diplomacy Toolbox; Regulation (EU) 2019/796; Decision (CFSP) 2019/797	The Cyber (Sanctions) (EU Exit) Regulations 2020	Autonomous Sanctions Act 2011; Autonomous Sanctions Regulations 2011
Scope	Global; targets individuals / entities engaged in malicious cyber activities	Global: targets individuals / entities responsible for cyberattacks threatening the EU or its member states	Global; targets individuals / entities involved in cyber activities undermining the UK's security or international organizations	Global; targets individuals / entities involved in significant cyber incidents
Sanctions Measures	Asset freezes, financial restrictions, travel bans	Asset freezes, travel bans, prohibition on making funds available	Asset freezes, travel bans, prohibition on making funds available	Targeted financial sanctions, travel bans
Enforcement Bodies	Office of Foreign Assets Control (OFAC)	European External Action Service (EEAS); Council of EU	Office of Financial Sanctions Implementation (OFSI)	Department of Foreign Affairs and Trade (DFAT)
Recent Developments	Sanctions against North Korean and Russian actors for ransomware campaigns like NotPetya and WannaCry	Regulation (EU) 2024/2642 and Decision (CFSP) 2024/2643 adopted on 8 October 2024 concerning restrictive measures in view of Russia's hybrid, destabilizing activities	Implementation of The Cyber (Sanctions) (EU Exit) Regulations 2020 post-Brexit	Establishment of an autonomous cyber sanctions regime in December 2021

2.2 Moreover, sanctions for some cyberattacks are now a part of more comprehensive sanctions regimes. A good example is the EU sanctions framework against those responsible for destabilizing activities against the EU and its member states. It allows to respond to hybrid attacks in a systematic manner.

On 8 October 2024, the EU adopted Regulation (EU) 2024/2642[30] and Decision (CFSP) 2024/2643[31], establishing a framework for restrictive measures in view of Russia's destabilizing activities. These legal instruments provide the basis for imposing sanctions on individuals and entities responsible for actions that threaten the EU and its member states, including cyberattacks. This new framework is rooted in the Strategic Compass for Security and Defense[32], approved by the Council in 2022, which called for the EU Hybrid Toolbox to detect and respond to hybrid threats.

The toolbox, operational since December 2022, highlights the EU's commitment to counteracting complex cyber operations through cohesive measures.

The EU's new framework targets individuals and entities who are responsible for, implementing, supporting, or benefitting from actions or policies by the Government of the Russian Federation that undermine or threaten democracy, the rule of law, stability or security in the Union, or one or several of its Member States, in an international organization or a third country, or which undermine or threaten the sovereignty or independence of one or several of its Member States, or a third country, through engaging in cyberattacks that have a significant impact on critical infrastructure, essential services, or public safety.

Restrictive measures include travel bans and asset freezes. The EU's comprehensive sanctions framework may serve as a model for other countries seeking to address hybrid threats, including cyberattacks. By establishing precise legal instruments and criteria for imposing sanctions, countries can enhance their resilience against destabilizing activities. Adopting similar frameworks would involve:

- Developing legal instruments that define the scope and criteria for sanctions.
- Establishing mechanisms for the identification and designation of individuals and entities responsible for destabilizing activities.
- Ensuring coordination with international partners to enhance the effectiveness of sanctions[33].

Expanding the EU's sanctions regime to address activities by other states, such as China, would require careful consideration of geopolitical dynamics and existing international relations.

The EU has previously expressed concerns regarding malicious cyber activities originating from Chinese territory. For example, in July 2021, the EU issued a declaration urging Chinese authorities to take action against malicious cyber activities undertaken from its territory[34].

Thus, this new regime could be expanded in two ways:

- The EU itself may use it against other countries, not only Russia.
- Other Western countries may incorporate this practice.

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2642
[31] https://eur-lex.europa.eu/eli/dec/2024/2643/oj
[32] https://www.consilium.europa.eu/en/policies/strategic-compass
[33] https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/russia-eu-sets-up-new-framework-for-restrictive-measures-against-those-responsible-for-destabilising-activities-against-the-eu-and-its-member-states/
[34] https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/

2.3. At least three tendencies are affecting the future of cyber sanctions.

First, Western countries will likely apply two-step attribution when announcing new sanctions – to a hacker group and a state. A recent study has demonstrated[35] that the EU was using more direct statements concerning the Russian involvement. For example, the declaration was issued in July 2022, recalling the condemnation of cyberattacks in January and the attribution of the KA-SAT attack to the Russian Federation in May 2022[36]. However, the EU still failed to mention that its members were affected. Nevertheless, this public statement can be interpreted as assigning direct state responsibility for a cyber operation. This step could be considered positive, as it enables comprehensive state responsibility.

Second, there will be a step-by-step transition from exclusively personal sanctions to sectoral sanctions. The apparent aim is limiting access to Western technologies that allow cyberattacks against critical infrastructure. Moreover, considering cyberattacks as an integral part of hybrid operations will bring about intersectoral restrictions. This approach is especially relevant in today's landscape, where advanced technologies – such as high-performance computing, artificial intelligence, and encryption tools – are critical enablers of malicious cyber activities.

Third, more coordinated actions are expected. For example, in October 2024, the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated seven individuals and two entities associated with the Russia-based cybercriminal group in a tri-lateral action with the United Kingdom's Foreign, Commonwealth & Development Office (FCDO) and Australia's Department of Foreign Affairs and Trade (DFAT)[37]. It's a good example of unified measures.

In July 2024, Australia, the United States, and six other allies issued a joint advisory identifying a Chinese state-sponsored hacking group as a significant threat to their networks. This unprecedented collaboration underscores the necessity for unified international efforts to combat cyber threats.

[35] https://eurepoc.eu/wp-content/uploads/2024/02/Right-Thoughts-Right-Words-Right-Actions-February-2024.pdf
[36] https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/
[37] https://home.treasury.gov/news/press-releases/jy2623

3. COMBATING CYBER AGGRESSION: RESPONSIBILITY AND PREVENTION

3.1. The responsibility for aggression shall be multidimensional, incorporating personal criminal responsibility and international legal responsibility of states.

Cyber aggression consists of two components: internationally wrongful acts by the Russian Federation and international crimes committed by the Russian military and political leadership. It should be particularly emphasized that cyber aggression violates erga omnes obligations. As the International Court of Justice has defined[38], these are the obligations in whose fulfilment all states have a legal interest because their subject matter is of importance to the international community as a whole. Thus, every state, not only Ukraine, can hold Russia accountable for violating these rules.

Whatever form the legal framework takes, expanding the definition of "aggression" to adequately address cyber threats is a crucial imperative. The current definition of "aggression" in international law is old-fashioned. In turn, not every cyberattack can be considered an act of aggression, even if the state directly organizes it. Two criteria shall be assessed: first, the scale of the cyberattack, and second, the intent to harm the sovereignty of another state.

Although a decision as to when a cyberattack would lead to the invocation of the NATO Treaty's Article 5[39] defense provision would be taken by the North Atlantic Council on a case-by-case basis, NATO affirms[40] that a cyberattack "impact could be as harmful to modern societies as a conventional attack" and that "cyber defense is part of NATO's core task of collective defense."

The scale of the attack can be measured by concrete consequences, such as its human victims or property damage. Respecting attacks on critical infrastructure, not only the destruction of the infrastructure itself but incapacitation for a considerable time should be considered in an aggression analysis. Intent to violate sovereignty should refer to the political will to commit an attack to harm the political independence or territorial integrity of another State.

Just as unfriendly incidents at physical borders are distinguished from full-scale war, isolated small cyberattacks are distinguishable from cyber aggression. However, deliberate infliction of tangible harm on another State through a cyberattack should be considered aggression, similar to the shelling of sovereign territory[41].

It is essential to advocate for a modernized definition of aggression in international law that reflects the unique nature of cyber warfare. One of the first steps may be inclusion of cyber domain into the jurisdiction of the special tribunal for the crime of aggression against Ukraine, capable of delivering justice by holding accountable those who bear the greatest responsibility[42].

[38] https://www.icj-cij.org/case/50
[39] https://www.nato.int/cps/en/natolive/official_texts_17120.htm
[40] https://www.nato.int/cps/en/natohq/official_texts_112964.htm
[41] https://ukraineverstehen.de/cyberaggression-braucht-das-voelkerrecht-ein-update/
[42] https://www.coe.int/en/web/portal/-/justice-for-crimes-committed-in-ukraine-ministers-of-justice-discuss-legal-cooperation-and-a-special-tribunal-for-the-crime-of-aggression

Aggression may be followed by other international crimes involving cyber elements. Further developments of the technologies create new possible threats:

- Genocide: emerging technologies and AI could be weaponized to commit genocidal acts, with cyberattacks playing a role in this process (above all, incitement to genocide).
- Ecocide: cyberattacks against critical infrastructure could potentially lead to significant environmental harm.
- Crimes against humanity: combined hybrid actions could establish a large-scale attack against civilians.

3.2. Some Russian cyberattacks can be qualified as war crimes. It means that Western companies enabling these attacks are assisting the commission of international crimes.

Under Article 25 of the Rome Statute[43] individuals may be criminally responsible and liable to punishment if they act to facilitate the commission of crimes and provide the means for their commission. This principle is also incorporated in the national legislation of many countries.

Prosecutors at the International Criminal Court are already investigating alleged Russian cyberattacks on Ukrainian civilian infrastructure as possible war crimes. Thus, legal precedents are likely to be created. ICC Prosecutor Karim Khan has explicitly stated that "cyber-enabled crimes may fall within the ICC's jurisdiction if the requirements of the Rome Statute are met[44]." According to the media sources[45], the ICC team is examining attacks on infrastructure that endangered lives by disrupting power and water supplies, cutting connections to emergency responders, or knocking out mobile data services that transmit air raid warnings. Russia's efforts to target and degrade Ukraine's energy infrastructure have underscored the increasing integration of cyberattacks alongside conventional military operations aimed at critical infrastructure.

Since attribution is the biggest problem, it is more appropriate to classify those cyberattacks against civilian infrastructure that are part of a more significant attack (when a conventional attack and cyberattack occur simultaneously or sequentially) as war crimes. At the same time, the context is essential. The International Criminal Court has jurisdiction over war crimes, particularly when they are committed as part of a plan or policy or as part of a large-scale commission of such crimes. That is, proving logical connections between various attacks will facilitate attribution and qualification (cyberattacks on civilian infrastructure are not abstract but part of a broader plan). At the same time, it secures the Ukrainian hacker community. Ukraine does not have a policy or plan to commit large-scale war crimes. And for Russia, it is a way of conducting hostilities.

In turn, a recent Reuters investigation demonstrates a striking tendency[46]: despite the Russian hybrid war, private actors undermine national security strategies. Western technology companies, including Cisco, IBM, and SAP, are acceding to Moscow's demands for access to closely guarded product security secrets. Russian authorities requested Western technology companies to review the source code of security products, such as firewalls, antivirus software, and encryption tools,

[43] https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf,
[44] https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through
[45] https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/
[46] https://www.reuters.com/article/technology/under-pressure-western-tech-firms-bow-to-russian-demands-to-share-cyber-secrets-idUSKBN19E0XB/

before allowing these products to be imported and sold in Russia. These requests are framed as part of a security policy. However, such inspections enable the Russian government to examine the underlying source code – essentially the set of instructions that govern the fundamental operations of the software. It could allow Russia to identify and exploit vulnerabilities in the code, creating possibilities for espionage or cyberattacks against Western targets. These inspections involve Russia's Federal Security Service (FSB) and the Federal Service for Technical and Export Control (FSTEC), both of which have been implicated in cyberattacks against Western nations. Moreover, many Russian private actors conducting these reviews have documented ties to the military or intelligence sectors. For example, Echelon is one of several FSB-accredited testing centers. Its website highlights its recognition by Russia's Ministry of Defense for the "protection of state secrets." The situation is even worse, as Echelon was sanctioned by the Western governments[47]. Russia is leveraging its regulatory mechanisms to access critical technology, potentially weaponizing it for strategic advantage.

It is desirable to enhance the dialogue with private companies. Companies shall prevent the misuse of their products, particularly in ways that could enable cyberattacks and suppress democratic movements. Failure to comply should result in clear consequences, like fundamental privileges, such as access to government contracts or diplomatic backing in international markets. By imposing such measures, governments can signal that sanctions violations will not be tolerated.

3.3. Justice is important. But preventing future crimes is even more crucial. That is why we shall learn lessons from the Russian aggression and deprive the authoritarian regimes of the instruments to wage hybrid wars.

Russia's dependence on Western technology is its weakness, which can be used to win a hybrid war. For example, the Russian authorities have made several attempts to force state agencies and private companies to adopt Russian-made alternatives to foreign technologies. Government decisions have sometimes been ignored or circumvented, as companies and institutions prefer to use more reliable, higher-quality solutions, even if that means facing penalties or legal consequences[48]. Russia's inability to keep up with these changes could leave the country further isolated and less competitive in the years to come. This means that scaling these vulnerabilities can be regarded as an investment in global security. Efforts must focus on preventing cyber espionage, which allows Russia to steal Western technologies and circumvent existing sanctions.

Another vital step is blocking Russia's access to Western software and the latest technologies without distinguishing between military and civilian ones. This approach prevents the exploitation of dual-use technologies for cyberattacks or espionage. Additionally, a complete ban on Russian software should be enforced, as many products can be used for cyberattacks and surveillance. To this end, the software supply chain shall be under more control and scrutiny. It is also important to prevent countries from becoming dependent on Russian software, as this strengthens the soft power of authoritarian regimes and increases dependence on them. International cooperation can further isolate Russian companies from global supply chains, hampering their technological progress.

[47] https://home.treasury.gov/news/press-releases/jy2204

[48] https://www.business-humanrights.org/fr/latest-news/opinion-how-to-exploit-russias-addiction-to-western-technology/

Finally, it is crucial to prevent Russia from using cyber diplomacy to achieve its geopolitical goals. The practice of international relations shows that Russia often tries to initiate the development of new international rules for cyberspace. While not intending to adhere to these norms in the future, Russia is trying to limit potential responses to its malicious actions unilaterally. Therefore, Western states should take a leadership position in developing new international legal norms while simultaneously strengthening the instruments of responsibility and coercion. In addition, the use of new international treaties for the potential violation of human rights by authoritarian regimes cannot be allowed[49].

[49]https://usun.usmission.gov/explanation-of-position-of-the-united-states-on-the-adoption-of-the-resolution-on-the-un-convention-against-cybercrime-in-ungas-third-committee/

CONCLUSIONS AND RECOMMENDATIONS

The cyber domain is an integral part of Russian aggression – not only against Ukraine but against all democratic states. Moreover, cyberattacks are used by China, Iran, and North Korea to achieve their national goals and undermine global security. Thus, international architecture shall be rearranged in accordance with modern challenges:

- The current punishment-based deterrence policy is not enough. All instruments shall be more coordinated and proactive. New restrictive measures shall be developed to deprive authoritarian regimes of the modern technologies and instruments to launch and maintain cyber aggression. A proactive strategy should not only be about punitive measures but also about building robust defenses within infrastructure, institutions, and through international collaboration. Continuous intelligence sharing, cross-border exercises, and real-time threat assessments should be prioritized to create a genuinely preemptive cyber defense posture.
- Western countries shall fully coordinate and synchronize sanctions regimes introduced to confront cyber warfare. Moreover, cyberattacks should be attributed to states in a more sustainable manner.
- At least some cyberattacks shall be regarded as a part of bigger threats – either conventional or hybrid. Sanctions shall target not only cyber or technological sectors but ensure a comprehensive influence on the ability to wage war or proceed with unlawful interference (the scope could be extended to explicitly target supply chains, financial systems, and logistical networks that indirectly support cyber aggression).
- New international legal approaches shall be implemented. The legal definition of aggression shall include the cyber domain, enabling responsibility of the Russian leadership for its crimes. Moreover, national and international courts, including the International Criminal Court, shall consider the legal qualification of some cyberattacks as war crimes.
- Modern security strategies and defense agreements should take into account cyber threats. Western countries should develop a clear vision of collective self-defense to address cyber aggression. It should include specific triggers for response, such as invoking Article 5 of NATO’s treaty in response to cyberattacks that threaten national security. Joint cybersecurity response teams could be stationed in member states to respond rapidly to transnational cyber incidents.
- Expanding beyond Western nations to include emerging economies in Asia, Africa, and Latin America is vital for a global approach. Authoritarian regimes often exploit vulnerabilities in these regions for cyber operations or use them as indirect hubs for cyberattacks. Building partnerships with these regions through capacity-building programs, technology transfer, and joint threat intelligence initiatives would broaden the impact and reduce safe havens for cyber aggression.