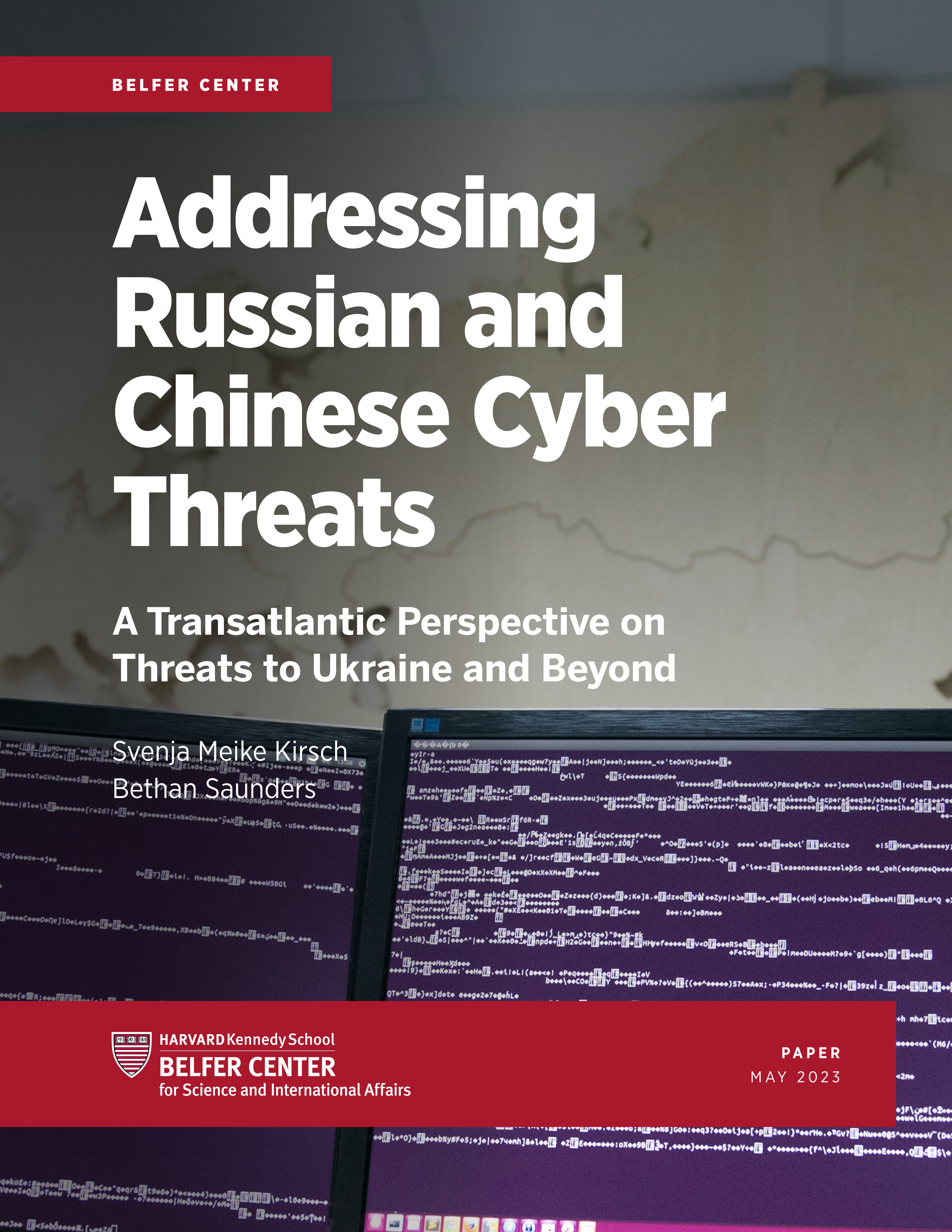


BELFER CENTER

Addressing Russian and Chinese Cyber Threats

A Transatlantic Perspective on Threats to Ukraine and Beyond

Svenja Meike Kirsch
Bethan Saunders

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2023

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

Statements and views expressed in this report are solely those of the author(s) and do not imply endorsement by Harvard University, Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

The designations employed and the presentation of the material on the maps in this report do not imply the expression of any opinion whatsoever concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

BELFER CENTER

Addressing Russian and Chinese Cyber Threats

A Transatlantic Perspective on Threats to Ukraine and Beyond

Svenja Meike Kirsch
Bethan Saunders

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2023

About the Authors

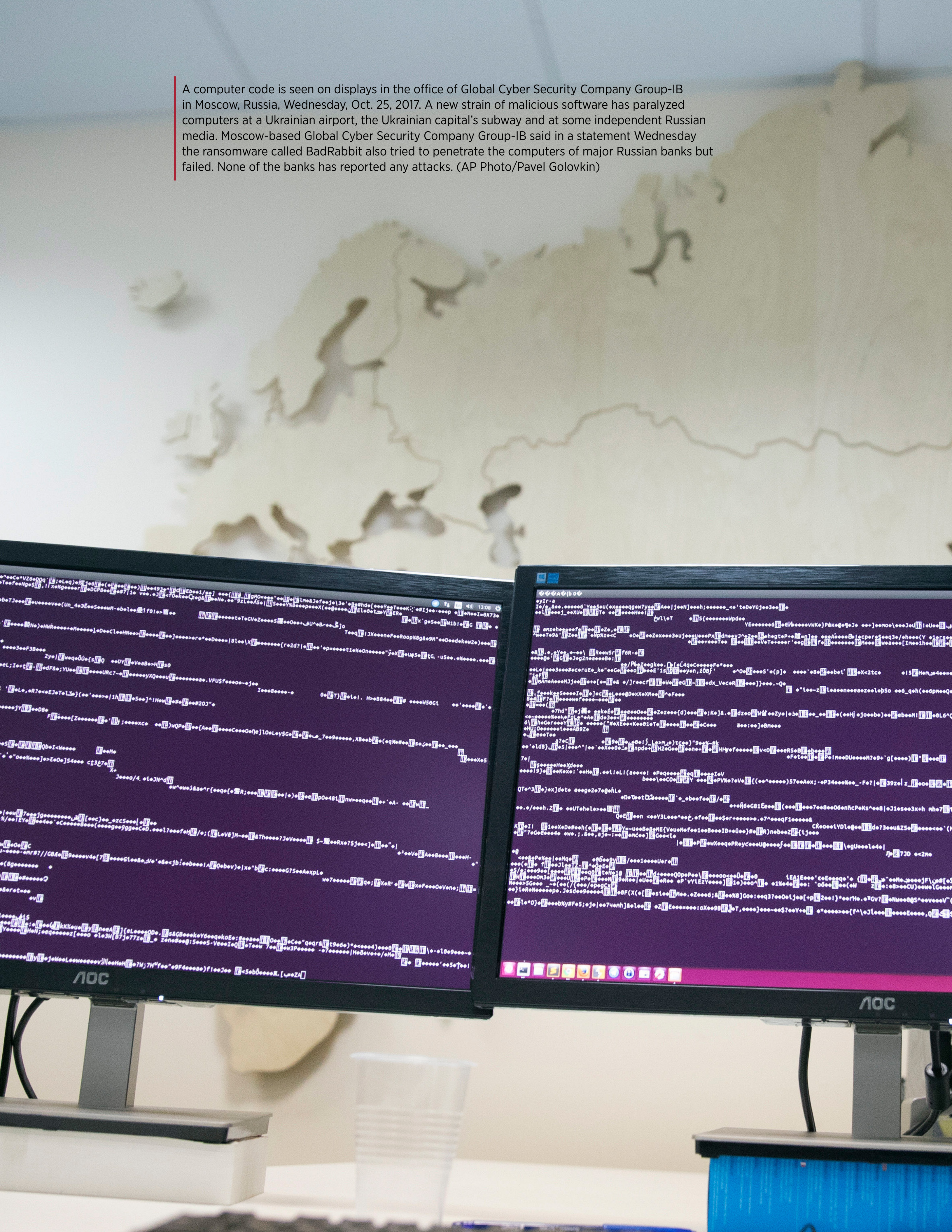
Svenja Meike Kirsch is a Fellow with the Defense Project and Project on Europe and the Transatlantic Relationship at the Harvard Kennedy School's Belfer Center. Her research focuses on the future of European security amid the Russian invasion of Ukraine. She is interested in the future role of NATO and the EU, implications of Russia's war for the international order, the role of the private sector as a safeguarding force of economic freedom, paths to European energy independence, and challenges facing liberal democracies given the rise of illiberal forces. Prior to joining the Belfer Center, Kirsch was a Fulbright and DAAD scholar at Harvard Kennedy School from which she earned a Masters in Public Policy. Her experience includes positions in sustainability management, social mission consulting, political campaigning, and think tank research. She holds a Bachelor of Arts in International Relations with a minor in Global Economics and Management.

Bethan Saunders is a second-year Master in Public Policy candidate at the Harvard Kennedy School, focusing on the intersection of national security, technology, and innovation. Bethan is the Co-Chair of the Harvard Kennedy School student organization, Women in Defense, Development, and Diplomacy, and a student coordinator for the Cambridge Project, which pairs graduate students with the Defense Innovation Unit on projects to accelerate commercial technology for national security. Bethan was also a Rosenthal Fellow on In-Q-Tel's Strategic Issues team. Before joining the Kennedy School, Bethan was an associate at Morgan Stanley, where she focused on business growth strategy, impact investing, and technology. She received her BSFS in International Politics and Security from Georgetown's School of Foreign Service.

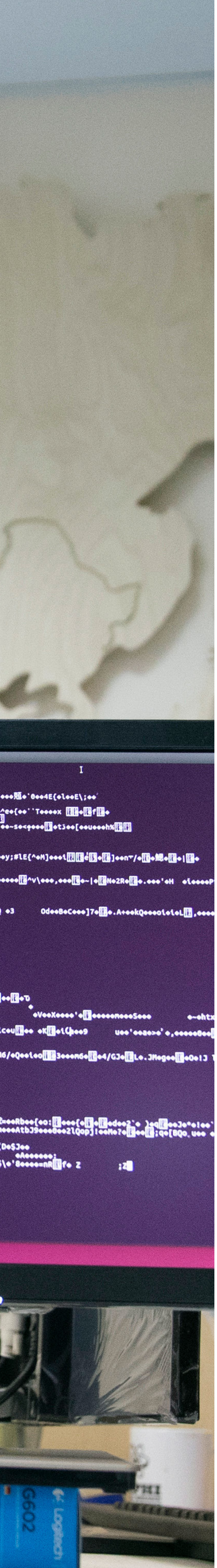
Acknowledgments

We would like to extend our gratitude to Eric Rosenbach, Co-Director of the Belfer Center, and Lauren Zabierek, former Executive Director of the Belfer Center and current Senior Policy Advisor at CISA. Your expert guidance, deep knowledge on cyber, thoughtful feedback, and support throughout our research provided a tremendous source of inspiration. We also want to thank Erika Manouselis, Research and Administrative Manager of the Project on Europe and the Transatlantic Relationship. Your expertise on transatlantic relations, international cooperation and academic research was incredibly helpful and substantially contributed to bringing this project across the finish line. Thank you also to Nicolas Cimarra Etchenique, Spanish Diplomat and Fellow at the Project on Europe and the Transatlantic Relationship. Lastly, we would like to thank the Belfer Center and the Project on Europe and the Transatlantic Relationship for centering and elevating our voices within international security, cyber policy, and transatlantic relations. We are very grateful to be a part of this community.

Table of Contents



A computer code is seen on displays in the office of Global Cyber Security Company Group-IB in Moscow, Russia, Wednesday, Oct. 25, 2017. A new strain of malicious software has paralyzed computers at a Ukrainian airport, the Ukrainian capital's subway and at some independent Russian media. Moscow-based Global Cyber Security Company Group-IB said in a statement Wednesday the ransomware called BadRabbit also tried to penetrate the computers of major Russian banks but failed. None of the banks has reported any attacks. (AP Photo/Pavel Golovkin)



Executive Summary

In an interconnected world, cyberattacks are becoming more frequent and sophisticated. Building resilience against this asymmetric threat is critical for countries to protect their economies, critical infrastructure, and democratic institutions. However, cyberattacks do not respect borders, and no country can address this threat alone. The strength and longevity of the transatlantic partnership between the EU and the U.S. presents a unique opportunity to address this strategic threat through international cooperation. Through an analysis of cyberwarfare in the ongoing war in Ukraine, this paper proposes policy recommendations to enhance transatlantic coordination and cooperation against current and future adversaries in a new era of strategic competition. Ultimately, a stronger transatlantic partnership is critical for protecting international democratic norms, building resilience against cyber threats, and strengthening global security and stability.

This paper addresses and presents policy recommendations for two significant challenges:

- **Challenge 1:** Curtailing Russia's ability to support war ambitions in Ukraine
- **Challenge 2:** Defending the transatlantic partners against the Chinese cyberwarfare threat

A Transatlantic Approach: This paper views these two challenges through the lens of the transatlantic partnership. As the geopolitical threat landscape has evolved in the 21st century, the transatlantic alliance is entering a new decisive era that could determine the future of global security and norms in cyberspace. The ongoing war in Ukraine has put significant pressure and elevated the importance of the transatlantic alliance to respond to Russia's blatant violation of international norms and human rights abuses. It has become clear that the U.S. and EU leaders must continue to work together to address threats to global stability, including the proliferation of cyberattacks as part of Russia's strategy in Ukraine, and China's efforts to undermine international democratic norms and alliances.

The new threats emerging from the increase in gray zone warfare from adversaries demonstrates how the relationship between the U.S. and the EU is even more essential for addressing threats that do not respect borders and have significant global implications.

Challenge 1: Curtailing Russia's ability to support war ambitions in Ukraine

For decades, Russia has used cyberattacks to destabilize the global community. Since the illegal annexation of Crimea in 2014, these attacks have grown in frequency, scale, and impact.[1] As one prominent example, U.S. Intelligence findings attribute the cyber-enabled spreading of disinformation and state-sponsored interference in the 2016 Presidential Elections to Russia.[2] Given the ongoing war in Ukraine and the potential role that cyberwarfare could play in advancing the Kremlin's territorial ambitions, further analysis of destructive capability and deterrence best practices are required.

Challenge 2: Defending the transatlantic partners against the Chinese cyberwarfare threat

While Russia remains an immediate threat to stability and security in cyberspace, the U.S. Department of Defense has described China as the "pacing" and primary long-term strategic threat for the EU and U.S. This means "that China is the only country that can pose a systemic challenge to the United States [...] economically, technologically, politically and militarily."[3] Recognizing that Russia's relative global power is declining in the medium- to long-term, understanding and leveraging best practices for transatlantic coordination from the ongoing war in Ukraine will be critical for addressing the strategic threat of Chinese cyber capabilities.

Policy Recommendations

This research aims to provide a starting point for proposing policy solutions for effective transatlantic cyber defense cooperation against common adversaries, most notably Russia and China. Together, the EU and U.S. can foster conditions for limiting the destructive impact of cyber-attacks in future conflicts and in a new

[1] Westby, J. (2020, December 20). Russia Has Carried Out 20-Years Of Cyber Attacks That Call for International Response.

[2] U.S: Senate Select Committee on Intelligence (2018, May 8). Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security

[3] Garamone, J. (2021, June 2). Official Talks DOD Policy Role in Chinese Pacing Threat, Integrated Deterrence

era of strategic competition. Collectively, the recommendations that this report advances will be critical for building a stronger transatlantic partnership to build resiliency against cyber threats, protect democratic norms, and strengthen global security and stability.

Recommendations: Curtailing Russia's ability to support war ambitions in Ukraine through cyber

- **The European Commission and the U.S. government should:**
    a. Formulate more **far-reaching, coordinated requirements for social media companies** to battle Russian disinformation;

    b. Incentivize **Western media to increase focus on detailing the horrors of war**;

    c. **Facilitate the creation of an international body** that institutionalizes big tech cyber support with help of the State Department's Bureau of Cyberspace and Digital Policy and its Bureau of International Organizations;

    d. Create a task force for **deeper intelligence sharing between the European Union Agency for Cybersecurity (ENISA) and Cybersecurity & Infrastructure Security Agency (CISA)**.

- **The Ukrainian government should:**
    a. Support **eastern Ukrainian media outlets with financial and political incentives** that disincentivize the spreading of disinformation;

    b. Focus immediate action on **better coordinating hacktivist groups and emphasize the rejection of counter-attacks**;

    c. Lead the movement for **an international organization institutionalizing big tech support** and providing **in-kind cyber support** for governments under attack;

    d. Encourage the **build-up of in-house cyber defense** of private and public entities;

e. Focus longer-term action on **mandates requiring minimum cybersecurity standards** for public and private entities;

f. Re-construct an **electricity grid whose design is less vulnerable to cyberattacks**.

Recommendations: Defending the transatlantic partners against Chinese cyberwarfare

- **The European Commission and the U.S. government should:**

  a. Establish transatlantic **cyber liaison roles**, introduce and expand personnel and cyber **workforce exchange**, and **align critical infrastructure cybersecurity standards** through the U.S.-EU Trade and Technology Council (TTC);

  b. Institutionalize **public-private partnerships** and collaboration by facilitating **transatlantic information sharing and analysis centers** (ISACs), prioritizing private sector information sharing, and creating **joint responses to Chinese cyber espionage;**

  c. Create an **EU-U.S. cyber capabilities fund** to support cyber and internet capacity building in developing countries;

  d. Launch an **awareness campaign about the importance of international norms in cyberspace** and **support the creation of dedicated norms-building mechanisms** by empowering efforts like the Paris Call and OECD Global Forum on Technology;

  e. **Coordinate technical standards-based policy and regulation** by engaging the U.S. in the creation of the EU's Cybersecurity Certification Commission and establishing a transatlantic working group with ENISA.

Introduction

Since the 2014 annexation of Crimea, Ukraine has been at the forefront of Russian cyberattacks. These have created real-world impacts, including disrupting electricity, and heating supply, and limiting information access. Since the full-scale invasion of Ukraine, Russian cyberattacks have been a constant feature. The combination of such attacks with missile strikes can have a detrimental impact on already dire living conditions and morale. Although no "big bang" destructive cyber efforts have been successfully rolled out, it is the multitude of attacks and their consequences accompanying military operations that haunt Ukraine. Given potential for more far-reaching attacks, it is pivotal that the EU and the U.S. learn from Ukraine's experience and shield their infrastructure.

This paper also seeks to address long-term challenges arising from other powers with well-developed cyber capabilities like China. As a "pacing threat" for international democratic norms, any transatlantic attempt to address cyberwarfare must address the long-term risks arising from China's rapidly growing cyber capabilities.[4] Given strong political will to respond to China's influence, there are several ways in which the transatlantic partners can improve their cyber cooperation. Strategic coordination is critical for maintaining U.S. and EU leadership in cyberspace and reducing China's ability to use cyber as an effective tool of hybrid warfare in a possible great power conflict.

Although conventional wisdom considers cyberwarfare mostly absent from Russia's war strategy,[5] the authors argue the Kremlin attempts to leverage it to further its expansionist agenda and influence public opinion.[6] However, Russia's performance in cyberspace is just as disappointing as its battlefield performance. Policymakers should not assume that cyberwarfare will represent the most effective future war capability because if effective defenses are built, cyberwarfare won't shape war outcomes.

[4] Garamone, J. (2021, June 2).

[5] Menn, J., Timberg, C. (2022, February 28). The dire predictions about a Russian cyber onslaught haven't come true in Ukraine. At least not yet.; Russia Matters (2022, May 4). Why Hasn't Russia Unleashed "Cybergeddon" in Its War on Ukraine?.; Maj Gen PK Mallick, VSM (2022). Decoding Russia's "Missing" Cyberwar Amid War in Ukraine; Carvin, S. (2022, September 22). Is Ukraine the Cyberwar That Wasn't

[6] Although disinformation campaigns represent a larger issue than just one related to cyber warfare, the authors refer to them whenever they are cyber-enabled. The authors recognize that tackling issues arising from disinformation require more than just cyber approaches.

Background

Russian Cyberattacks on Ukraine Prior to the Full-Scale Invasion

Information operations and disinformation, alongside cyber operations, play a key role in Russian attempts to discredit Ukraine's sovereignty and its government. Russia has long-used gray zone tactics (i.e. tactics that fall "in between routine statecraft and direct and open warfare," even prior to its full-scale invasion of Ukraine).[7] Ukraine has been one of the most popular targets of Russia's cyberattacks. Since at least May 2014, many of Ukraine's critical infrastructure industries, including electricity providers, railway operators, broadcasters, and energy companies, as well as regional governments, were targets of Russian hacking. Often, these attacks were launched in support of Russian-backed separatists in eastern Ukraine, who led war efforts against Ukraine since 2014.[8]

An example illustrating the severity of these incidents provides a December 2015 attack on Ukraine's electric grid. This attack left parts of the country without power for several days.[9] Given the timing of the attack during a cold winter, it is evident that Russia's intention was to instill fear in the civilian population and that the attackers were willing to risk the loss of human life. Another intention the alleged Russian interference with the 2014 and 2019 Ukrainian elections exemplifies, appears to be political destabilization. As a result of these cyberattacks, the Ukrainian Central Election Commission was compromised in 2014. In 2019, attempts at compromising the Commission failed, but disinformation was spread through social media, and then-presidential candidate Zelensky's official website was temporarily sent offline.[10]

Russia's mastery of gray zone tactics can be exemplified through the 2017 *NotPetya* malware attack. The attack mainly targeted the Ukrainian private sector and the country's government with a commonly used tax software, which spread malware and led to data destruction.[11] The attack spread across Europe, the Americas, and

[7] CSIS International Security Program (2019, July 8). By Other Means: Campaigning in the Gray Zone.

[8] Geers, K. (2020). Case Study: Defending Democracy in Ukraine. In Alliance Power for Cybersecurity, 11-16.

[9] Gordon, S., Rosenbach, E. (2021, December 14).

[10] Geers, K. (2020).

[11] Council on Foreign Relations (n.d.). NotPetya.

Asia, causing more than $10 billion USD in economic damages globally.[12] It crippled multinational companies with nine-figure costs, and even spread back to Russia, hitting the state-owned oil company Rosneft. Although multiple transatlantic partners attributed the attack to Russian state-sponsored actors, the Russian government denied the accusations. It has since been undeterred by international condemnation concerning its aggression in cyberspace.[13] Given the widespread nature of the attack, *NotPetya* demonstrates the urgency for stronger transatlantic cyber capabilities for rapidly and effectively responding to cyberattacks from rogue actors like Russia.

Prior to the full-scale invasion, Russian attackers focused on military and strategically important targets such as facilities for military equipment. The destruction of these targets had the potential to reduce short-term Ukrainian military capability. This was illustrated with attacks aimed at Ukrainian Army Rocket Forces and Artillery, which caused the destruction of 80% of Ukrainian D-30 long-range Howitzers. Attackers developed an application through which intelligence analysts could gain access to Ukrainian military communications. This allowed them to identify the whereabouts of artillery and other equipment, while reducing targeting time per D-30 to under 15 seconds.[14] Apart from the severity, political sensitivity, and strategic targeting of some attacks, it is the sheer amount of Russian-led cyber intrusions that stand out. Between October and December 2016 alone, Ukraine witnessed over 6,500 cyberattacks on 36 targets, most of them associated with Russia's intelligence agency.

Between October and December 2016 alone, Ukraine witnessed over 6,500 cyberattacks on 36 targets, most of them associated with Russia's intelligence agency.

[12] Reuters (2018, February 15). White House blames Russia for 'reckless' NotPetya cyber attack.

[13] Council on Foreign Relations (n.d.). NotPetya.

[14] Seward, S. J. (2018). Cyberwarfare in the Tactical Battlespace: An Intelligence Officer'sPerspective. Fort Benning: US Army Fort Benning and the Maneuver Center of Excellence.

The Evolution of the EU's Cybersecurity Landscape

Since most of the EU cyber infrastructure and strategy was established in the last decade, the focus of this section lies on analyzing the EU's efforts in cyberspace, including its policies, institutions, and challenges. While NATO plays a critical role in defining the transatlantic relationship, there is a lot to be learned about building a more secure, stable, and integrated cyberspace through EU-U.S. coordination. NATO inherently lends itself to close coordination given the U.S. leadership role and definition of cyber as the "new frontier of Democratic Self-Defense".[15] However, building closer ties and strategic coordination between the EU and U.S. beyond NATO presents novel hurdles.

The EU made significant strides in building cyber strategy in recent years, remedying a historic lack of institutional and strategic direction in the sphere. Before the EU committed to centralizing cybersecurity and creating an institutional infrastructure in the 2010s, cybersecurity-related matters were the responsibility of each member state. Given its membership model, the EU also must overcome the unique challenges of equalizing cyber capabilities and resiliency across different member states that have disparate capabilities, and that face different threats.

The EU created its first cybersecurity strategy in 2013. Since the EU *General Data Protection Regulation* (GDPR) came into being in 2018, the regulations targeting technology and cybersecurity increased, with key milestones being the passing of various acts. Among them are the *Network and Information Systems Directives* 1.0 and 2.0 (NIS1 and NIS2), the 2019 *Cybersecurity Act*, the 2022 *Data Governance Act*, and the proposed Cyber Resilience Act.[16]

In 2020, the European Commission presented the EU's latest Cybersecurity Strategy. This strategy focuses on: 1) resilience, technological sovereignty, and leadership; 2) operational capacity to prevent, deter and respond; and 3) cooperation to advance

[15] Zabierek, L. (2022). The New Frontier of Democratic Self-Defense

[16] NIS1 and NIS2 are EU-wide pieces of legislation that aim to achieve a high level of cybersecurity across EU member states. The Cybersecurity Act is a regulation that gave the EU's cybersecurity agency ENISA a permanent mandate and that introduced a uniform European certification framework for information and communication technology products, services, and processes. The EU's 2022 Data Governance Act aims to increase trust in data sharing, improve its availability and support the creation of common European data spaces. The Cyber Resilience Act, which still needs to be passed, proposes to impose cybersecurity obligations on all products with digital elements that want to enter the EU market.

a global and open cyberspace.[17] The strategy aims to address the legacy of the membership model and prioritizes building collective capabilities for more robust cyberattack responses. It highlights the importance of partnerships to ensure stability in cyberspace and emphasizes the EU's leadership ambition in cyber standard setting. Through this strategy, the European Commission charted a path for deeper integration related to cybersecurity.

The strategy recognizes that the EU ecosystem does not have a centralized mechanism for cybersecurity communities to coordinate. To address this, the EU will create the *Joint Cyber Unit* (JCU). Once operational, it will bring civilians, law enforcement, diplomatic, and cyber defense communities together to prevent, deter and respond to cyberattacks. With a mission built on partnership, the JCU represents opportunities for transatlantic engagement.[18]

To strengthen the EU's cybersecurity ecosystem, the *European Cybersecurity Competence Centre* (ECCC) was established in 2021. The ECCC facilitates coordination between EU member states' national cybersecurity competence centers (NCC).[19] The Centre's core responsibility is to coordinate cybersecurity research and innovation. It also centralizes EU investment in cybersecurity research and development.

The ENISA remains a central feature of the EU's cybersecurity landscape. ENISA was created in 2004, and its responsibilities continue to grow as the EU prioritizes cybersecurity, given the multitude of hostile cyber actions of Russia and China. The 2019 EU *Cybersecurity Act*, greatly strengthens the role of ENISA by giving it a permanent mandate. Prior to 2019, ENISA had a fixed-term mandate and was described as a "small agency with a low budget and staff compared to [other] EU agencies."[20] Today, ENISA has a stronger mandate for operational cooperation and crisis management.

ENISA will be in charge of implementing the NIS2 Directive, which provides a legal framework associated with the mandate to strengthen overall EU-level cybersecurity.

[17] European Commission (2022, June 7a). The Cybersecurity Strategy.

[18] European Commission (2022, June 7b). Joint Cyber Unit

[19] European Cybersecurity Competence Centre and Network (n.d.). About us.

[20] European Commission (2017, September 13). Proposal for a Regulation of the European Parliament and of the Council on ENISA , the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

The NIS2 Directive mandates a high common level of cybersecurity across the EU, with requirements for member states' preparedness, cooperation and information sharing through new "cooperation groups", and higher security standards for critical infrastructure and essential services.[21]

ENISA is the central agency for the ongoing EU-wide certification framework. Outlined in the *Cybersecurity Act*, this framework will be the first EU-wide cybersecurity certificate to limit risks posed by fragmentation between member states. Not only does the framework represent historic progress toward standardizing cyber measures, but it will also provide guidance to international businesses. However, the EU still needs to increase its response capacity to growing threats. ENISA is responsible for "achieving a high common level of cybersecurity across Europe",[22] but only has a staff of about 100 people. The U.S. can play an important role in helping the EU expand its cyber workforce, and ENISA is a key player for driving collaboration.

[21] European Commission (2023, January 16). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

[22] ENISA (2023). Supporting Policy Developments to Achieve a High Common Level of Cybersecurity.

Organization	Roles and Duties
European Union Agency for Cybersecurity (ENISA)[23]	• Assists the European Commission and EU members in meeting requirements of the NIS Directives by sharing information,best practices, and raising awareness • Establishes an EU-wide cybersecurity certification framework • Supports coordination of the EU response in the case of large scale, cross-border cyberattacks
European Union Military Staff (EUMS)[24]	• Supports development of cyber defense capability of member states to ensure protection in military operations
European Cybercrime Centre at Europol (EC3)[25]	• Strengthens law enforcement responses to cybercrimes • Functions as central hub for criminal information and intelligence, supporting criminal investigations • Raises awareness of cyber crimes
Computer and Emergency Response Team (CERT-EU)[26]	• Hosted within the Directorate-General for Informatics of the European Commission • Comprises information technology experts from EU bodies to share information, coordinate responses, and provide operational assistance
European Cybersecurity Competence Centre (ECCC)[27]	• Established to move implementation of the EU's Cybersecurity Strategy along • Facilitates coordination between EU member states' national cybersecurity competence centers (NCC) • Core responsibility is to coordinate EU- cybersecurity research and innovation
European Joint Cyber Unit[28]	• Aims to counter legacy of the EU's membership model on cybersecurity coordination and to complete commitment to collective cyber efforts • Will bring together civilians, law-enforcement, diplomatic, and cyber defense communities to prevent, deter and respond to cyberattacks • Set to be operational by June 2023
Stakeholder Cybersecurity Certification Group[29]	• Will be responsible for advising the Commission and ENISA on strategic issues regarding cybersecurity certification, and assisting the Commission in the preparation of the Union rolling work programme • First stakeholder expert group for cybersecurity certification in EU

[23] ENISA (2023).

[24] European Union External Action Service (2022, January 24). The European Union Military Staff.

[25] Europol (2022, March 1). European Cybercrime Centre - EC3.

[26] CERT-EU (2023). About us.

[27] European Cybersecurity Competence Centre (n.d.).

[28] European Commission (2022, June 7b).

[29] European Commission (2022, December 19). Stakeholder Cybersecurity Certification Group.

Evolution of EU-U.S. Cyber Coordination

With the rapid growth of global and hybrid threats, the U.S. and EU have committed to a resilient and strong cybersecurity partnership that prioritizes "an open, interoperable, secure, and reliable internet; and stability in cyberspace."[30] The partnership has been functional and normative, seeking to address joint vulnerabilities through cooperation, while committing to shared values and norms in cyberspace. Over the last decade, EU and U.S. principles converged on international cooperation, coordination with the private sector, balancing security, and fundamental human rights, and protecting the multi-stakeholder model of internet governance. These shared values were developed through bilateral and multilateral coordination. However, there have been policy differences on standards, privacy, and engagement with China's expansive telecommunications infrastructure efforts that have presented coordination challenges. Even with these differences, shared norms, principles, and regulatory frameworks help shape a common transatlantic cybersecurity identity.[31]

Established in 2010, the U.S.-*EU Working Group on Cybersecurity and Cybercrime* represents one of the first signals toward joint strategic coordination between the U.S. and EU. As the first transatlantic dialogue format, it addresses challenges related to cybercrime and cybersecurity and attempts to align standards while fostering cooperation. Since the launch of the working group, the U.S. and the EU elevated cybersecurity as a key issue in their bilateral relationship. The close links between the U.S. and EU economies have driven the prioritization of establishing shared cybersecurity standards, and interoperability of digital systems and platforms in key sectors.

The Biden administration has made strong commitments to a renewal of the transatlantic partnership and closer cooperation on cybersecurity, after a distancing during the Trump administration. In 2022, the Biden administration established the *Bureau of Cyberspace and Digital Policy* at the State Department. Since the Bureau's creation, efforts to support Ukraine's cyber defense are closely coordinated with the EU.[32] Held in December 2022, the Third TTC Ministerial Meeting and the eighth *EU-U.S. Cyber Dialogue* represent the most recent formal signaling of the continued

[30] U.S. Department of State (2022, December 21). The 2022 U.S.-EU Cyber Dialogue.

[31] Anagnostakis, D. (2021) The European Union-United States cybersecurity relationship: a transatlantic functional cooperation.

[32] U.S. Department of State (2022, May 10). U.S. Support for Connectivity and Cybersecurity in Ukraine.

collaboration on cyber threats. For the U.S. and EU, it is critical infrastructure security that is especially important. The U.S. and EU have also elevated support of Ukraine as a cornerstone of ongoing cybersecurity coordination.

In a joint statement from March 2022, Commission President von der Leyen and President Biden committed to "advancing our cooperation on cybersecurity through a variety of actions, from supporting the government of Ukraine on cyber resilience and cyber defense to aiming to combat the abuse of virtual currency."[33] Additionally, the new 2023 U.S. *National Cybersecurity Strategy*, stresses American commitment to leverage international partnerships on cyber and to develop new, collaborative law enforcement mechanisms. The strategy highlights strong support of models like the *European Cybercrime Centre*, which has been vital to modernize legal frameworks, train law enforcement, and collaborate with private sector partners.[34]

In a joint statement from March 2022, Commission President von der Leyen and President Biden committed to "advancing our cooperation on cybersecurity through a variety of actions, from supporting the government of Ukraine on cyber resilience and cyber defense to aiming to combat the abuse of virtual currency."

The U.S. and EU have also shown unity in shaping global cybersecurity standards within multilateral forums. Leaders from both sides recognize that their combined diplomatic and economic influence can lead to more effective norm-building. This understanding dates back to at least 2001, when the U.S. supported the promotion of the Council of Europe's *Budapest Convention*, one of the early landmark agreements on cybercrime and capacity building.[35] The U.S. and EU built on this Convention to promote common risk management criteria for the protection of critical digital infrastructure and global public-private partnerships.

On the international stage, the EU and U.S. have been close allies in condemning Russia and China's norms violations in cyberspace, and in advocating for a free and open internet. In 2021, the U.S. and EU co-sponsored a UN General Assembly resolution on "Advancing responsible state behavior in cyberspace in the context of

[33] European Commission (2022, March 24). Joint Statement by President von der Leyen and President Biden.

[34] The White House (2023, March 1). National Cybersecurity Strategy.

[35] Council of Europe (2001). The Budapest Convention (ETS no. 185) and its Protocols.

international security," which called for greater cooperation between states and the private sector to enhance cybersecurity. Both the EU and U.S. also support the work of the UN Group of Governmental Experts and the UN Open-Ended Working Group on producing norms for responsible state behavior in cyberspace.[36]

However, there have been significant divides in the U.S. and EU approaches to cybersecurity policy and internet governance. Although both share concerns about the threats posed by malicious actors in cyberspace and addressing digital risks and opportunities, the EU tends to prioritize regulation while the U.S. prioritizes innovation. As such, the EU has been more aggressive in enacting policies on privacy, antitrust, and digital taxation. In 2016, the EU enacted its historic *General Data Protection Regulation* (GDPR) law, which provides citizens with greater control over personal data. GDPR has far-reaching implications for U.S. citizens and companies, which many U.S. policymakers perceive as an overreach that constrains innovation outside the EU. The EU is also working on developing a digital tax, which would be determined on a company's EU revenue. However, this initiative has faced resistance from the U.S. based on arguments that it would unfairly target American companies.

In contrast to the EU's governance efforts, the U.S. has been more focused on the national security implications of new emerging technologies, such as artificial intelligence and 5G. In particular, addressing China's involvement in 5G networks and critical telecommunications infrastructure has been a source of tension between the U.S. and its EU partners. During the previous administration, former U.S. President Trump threatened to stop sharing intelligence with European partners should they continue using *Huawei* as the provider of their telecommunication needs. While aggressive, this hard-handed approach to 5G was successful, insofar as many EU member states placed restrictions on the use of *Huawei*-provided telecom networks.[37] The Biden administration maintains the ban on American companies working with *Huawei*, and continues to push allies to choose alternative telecommunication companies. U.S. efforts have led to more far-reaching European measures to protect communication infrastructure from Chinese influence, although the debate over the reliance on *Huawei* created a significant point of tension in the transatlantic relationship.

[36] Council on Foreign Relations (2022). Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet.

[37] Scott, M. (2021, February 4). How Trump Won Over Europe on 5G.

These divergent priorities and approaches may limit the effectiveness of transatlantic cooperation on tech policy, although both regions recognize the need to work together to address the challenges of the digital age. The EU and the U.S. continue to face a similar cyber threat landscape, and as a result, cyber capacity building through bilateral and multilateral means is central to EU-U.S. coordination. Key aspects of capacity building include situational awareness and information sharing, in addition to joint support on technical, operational, and political crisis management.[38] To this end, the EU and U.S. conduct joint cyber tabletop exercises to better coordinate capacity building and strengthen resiliency. However, the evolving threat landscape demands iteration of capability building.

Policy Challenge 1: Curtailing Russia's Ability to Support War Ambitions in Ukraine

To grasp the role of cyberwarfare in the Ukraine War, it is important to understand the Kremlin's aims and tools.[39] The actors behind these cyberattacks are thought to be Russian government-affiliated groups, pro-Kremlin hacktivists, and directly or indirectly Kremlin-funded entities.[40] As of late 2022, hacktivist groups account for the majority of incidents targeting Ukraine, estimated to be responsible for 91.4% of all recorded cyberattacks.[41] Recognizing the covert nature of many cyber operations, it is often hard to reliably attribute cyberattacks. For simplification, attacks referenced in this paper will be considered Kremlin-related. They fall into two areas of gray zone tactics, namely into cyber-enabled information operations and cyber operations. In the first area lies the spreading of disinformation. In the second area lie three additional tools: dismantling public and private software, espionage, and destroying critical infrastructure.

[38] European Commission (2022, December 16). Cybersecurity: EU holds 8th dialogue with the United States.

[39] Although Russia's cyberwarfare tactics are employed internationally to shape perception of the country's war in Ukraine favorably, and to discredit the Ukrainian government, this analysis focuses on what happened within Ukraine. It will not provide a discussion of the Kremlin's domestic efforts to prevent civilian upheaval and ensure support of the war. Although the focus lies on what has happened to Ukraine's cyber infrastructure as a result of Russian attacks and breaches, Russian "retaliatory" actions against the transatlantic partners that support Ukraine will be considered part of the Russian cyber toolkit.

[40] Sabbagh, D. (2023, January 19). Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency.

[41] CyberPeace Institute (2023). Cyber Dimension of the Armed Conflict in Ukraine. *Quarterly Analysis Report Q4 from October to December 2022.*

Information Operations

Tool 1: Cyber-Enabled Disinformation.

The weeks leading up to the invasion were characterized by Russian attempts to take control of the narrative in the international press. This state-controlled disinformation campaign focused on domestic stakeholders, neighboring countries, and other global players with the goal of influencing public opinion favorably and pre-empting major sanctions. The Kremlin aims to portray Ukraine and NATO as the aggressors, which is divorced from the brutal reality of Russian aggression in Ukraine. However, with the help of cyber tools, Russia is spreading assertions suggesting that Ukraine provoked Russian aggression by committing atrocities and even genocide in the Donbas.[42] This blame-shifting narrative continues to be promoted in cyberspace and co-exists alongside the kinetic war effort. Other false narratives the Russian government pushes include that Ukraine resells Western weapons, that Russian massacres like in Bucha are staged,[43] or that Nazi ideology is a key feature of Ukrainian life.[44] The Kremlin's goal appears to be to undermine Ukraine on all fronts, including harming morale, international trust, and financial, and military support. Some cyber tools that Russia employs to achieve this goal include deep fakes featuring Ukrainian leaders, disinformation, falsified imagery or documents, and fact-checking groups defending Russian crimes.[45]

More than 85% of Ukrainian respondents oppose any territorial concessions - a figure consistent with pre-war sentiments.

In the case of Ukrainian audiences, there is limited belief in Russian disinformation. Immediately after the outbreak of the war, record numbers of civilians, many without military experience, stepped up to defend their country - by taking up arms, or by protesting occupation, as seen in March 2022 in Kherson.[46] This attitude seems prevalent among Ukrainians of all generations, with people across age groups joining Ukraine's defense.[47] Evidence

[42] Delegation of the European Union to the PRC (2022, March 18). Disinformation About Russia's invasion ofUkraine – Debunking Seven Myths spread by Russia.

[43] Atlantic Council (2023). Undermining Ukraine: How the Kremlin Employs Information Operations to Erode Global Confidence in Ukraine.

[44] OECD (2022, November 3). Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses.

[45] Atlantic Council (2023).

[46] BBC News (2022, March 5). War in Ukraine: Thousands march in Kherson against occupiers.

[47] Erlich, A., Garner, C. (2023). Is pro-Kremlin Disinformation Effective? Evidence from Ukraine.

supporting this perception includes a December 2022 survey that identified that more than 85% of Ukrainian respondents oppose any territorial concessions - a figure consistent with pre-war sentiments.[48]

However, there is one important caveat: the differing perception of ethnic Russians with Ukrainian citizenship. Although research from 2021 featuring a culturally diverse group of Ukrainians confirms the perception that the average Ukrainian can distinguish Russian disinformation from truth, the same study also found ethnic Russians are more likely to believe Russian disinformation.[49] Anecdotal evidence from eastern Ukrainian cities like Lysychansk, which are increasingly isolated from Western media and constantly under fire, supports this finding. There, a growing number of residents believe Russian propaganda that shifts the blame for shelling on Ukraine.[50]

While the focus lies on Russian cyber efforts against Ukraine, the impact of the Kremlin's information operations on third-party countries' perception necessitates discussion. Mainstream Western media has, for the most part, contributed to public rejection of Russian narratives as justifications for the unlawful invasion of Ukraine. The exception are groups of far-left and far-right wing politicians and news outlets in countries like Bulgaria, Czech Republic, Germany, or Slovakia, which are calling for an end of direct military support of Ukraine. These groups also advocate for a diplomatic solution benefitting Russia.[51] Otherwise, it is the combination of far-reaching sanctions that de-facto exclude Russia from the Western economic system, and unprecedented military support of the EU and NATO that reinforce this argument. Although Russia continues to target Western audiences with disinformation, as evident in hacktivists' breaching of influential Polish social media accounts to spread falsehoods about a made-up Polish plan to send back refugees, they have limited success.[52]

In the Global South, public opinion seems to be on the Ukrainian side in principle. This becomes evident when considering that an overwhelming majority of 141 UN members voted in favor of a resolution condemning the invasion and demanding

[48] Fivenson, A., Petrenko, G., Víchová, V., Poleščuk, A. (2023). Shielding Democracy: Civil Society Adaptations to Kremlin Disinformation about Ukraine.

[49] Erlich, A. & Garner, C. (2023).

[50] Gibbons-Neff, T., Yermak, N. (2022, June 17). Russian Breached This City, Not With Troops, but Propaganda.

[51] Olterman, P. (2023, February 24). Leaders of German left condemn "peace rally" over far-right involvement.; France24 (2023, March 13). Ukraine war fears give eastern Europe's populists new ammo.

[52] Atlantic Council (2023).

immediate Russian withdrawal from Ukraine, both directly after the beginning of the invasion and one year into it.[53] However, support in principle does not imply support in practice. It also does not mean that Russian disinformation is ineffective.

Powerful examples of diverging practices include former Soviet Republics Armenia, Kazakhstan, and Uzbekistan, which abstained and witnessed a significant increase in exports to Russia following the invasion. India, the largest democracy on earth which also abstained, continues to uphold far-reaching trade relations with Russia and has even scaled up its oil imports. Brazil, Costa Rica, and Turkey, which voted in favor of the resolutions, likewise saw an increase in exports to Russia. It is also through third-party countries in non-compliance with international sanctions that Russia can exploit loopholes and shield its economy from the full force of sanctions.[54]

When it comes to China, the picture looks even worse. China has not just been receptive to Russian disinformation, but its government is also actively supporting the Kremlin's effort to make people around the world believe that not Russia, but NATO is the aggressor. According to U.S. intelligence, China does so by spending billions of dollars globally, much of it on cyber operations.[55]

Addressing Russian Information Operations

Many Ukrainian and Western policy responses to Russian cyber operations proved successful and Ukrainian narrative power seems for the most part unharmed by Russian disinformation. Recognizing that cyberattacks can be particularly effective when aimed at influencing public opinion, the challenge for the Russians is that the Ukrainian government gained control of the narrative early on. This is largely due to the American intelligence communities' repeated warnings about Russian military build-up, which helped debunk the Russian narrative and contributed to swift Western support for Ukraine.[56] It is also due to the Ukrainian government's ability to use social media as an effective tool to communicate directly with the world and the country's citizens. This ability exists alongside the determination of leaders across

[53] UN General Assembly (2022, March 2). Resolution adopted by the General Assembly on 2 March 2022 - Aggression against Ukraine.; UN News (2023, February 23). UN General Assembly calls for immediate end to war in Ukraine.

[54] Holder, J., Leatherby, L., Troianovski, A., Cai, W. (2023, February 23). The West Tried to Isolate Russia. It Didn't Work.

[55] Wintour, P. (2023, February 28). China spends billions on pro-Russia disinformation, US special envoy says.

[56] Nye, J. S., Jr. (2022, June 15). Eight Lessons from the Ukraine War. New York: Project Syndicate.

government levels to keep up the fight, which hinders Russia's ability to win hearts and minds.

Other factors that contribute to reducing the threat of Russian disinformation are pre-existing domestic efforts in Ukraine to strengthen the media landscape through professionalization reforms, and legislation mandating the disclosure of media ownership. There are also projects aimed at increasing the role of local news outlets that were helpful.[57] One of the targeted responses to Russian disinformation campaigns is fact checking on *Telegram* and *Twitter* through the newly established *Center on Countering Disinformation* (CCD). Established by presidential decree as part of the National Security and Defense Council of Ukraine, the CCD provides the public with examples of false content alongside information about military developments.[58] It also provides background on how disinformation strategies are designed to manipulate audiences and thereby helps improve media literacy - a key tool to fight disinformation at its roots. It is also the governments' attention to social media and its hands-on approach to managing the digital space through tools like the Ministry of Digital Transformation's chat bot on *Telegram*, that has proven effective. This chat bot provides users with the opportunity to send primary information through videos or locations of Russian troops, and helps support Ukrainian intelligence.[59]

Ukrainian efforts are supported internationally through organizations like the *National Democratic Institute* which created a platform featuring insights from civil society groups on disinformation. With the help of this platform, civil society can gain access to journalists and deepen understanding of localized Russian disinformation operations to then address them.[60] AI and machine-learning tools of organizations like *Texty* are also helpful as they allow for impact comparison of false narratives by identifying regions, where a specific narrative lands well. This information can help authorities focus counter efforts in a timelier manner.[61]

Other private organizations that support the fight against disinformation are social media outlets like *Facebook, Twitter, YouTube,* and *Telegram*, all of which took steps like account and group removal, banning Russian media channels, content deletion,

[57] OECD (2022, November 3).

[58] Verkhovna Rada of Ukraine (2021, March 23). About the creation of the Center for countering disinformation.

[59] OECD (2022, November 3).

[60] Fivenson et al. (2023).

[61] Fivenson et al. (2023).

or labeling disinformation. The EU, the European External Action Service, G7, NATO also stepped up in support of Ukraine by offering fact-checking, directly responding to false Kremlin narratives, offering information sharing tools, and providing technical expertise exemplified by the deployment of the EU's *Cyber Rapid Response Team*.[62]

Still more tools are needed to tackle the global problem of disinformation. One set of tools that the transatlantic partners should embrace entails stepping up domestic and international regulation of social media platforms. This is especially important for non-Western owned platforms like *TikTok* as they feature pro-Russian disinformation to a much larger extent than other outlets. Amid increasing transatlantic relevance of "Ukraine fatigue" due to the perceived economic and political costs of continued support of Ukraine, EU and U.S. policymakers should also incentivize news outlets to spotlight the horrifying evidence of Russian crimes even more. This can prove effective in retaining support of Ukraine and help discredit Kremlin-aligned fractions.

On the Ukrainian side, transparency about media sources of funding and ownership structures needs to increase further. Ukrainian policymakers should also create more financial, political, and industry incentives, which make spreading disinformation less attractive. Importantly, deeper cooperation across sectors is needed to combat disinformation head-on in a hyper-timely manner.

Recommendations: The EU Commission and U.S. government should revisit the EU's Digital Services Act to formulate more far-reaching transatlantic requirements for social media companies to battle Russian disinformation. They should incentivize Western media to increase their focus on detailing the horrors of war to mitigate the risk of growing domestic opposition to continued support of Ukraine.

- **Ensure commitment to U.S.-EU Policy alignment:** Given that the EU has been more open-minded towards regulating big tech than the U.S., the initial focus will lie on getting the U.S. on board with the proposal. The European Commission should present the U.S. government with an impact assessment that documents the success, although not far-reaching enough, of the *Digital Services Act* on combatting disinformation. *TikTok* should be

[62] OECD (2022, November 3).

used as a reference case to convince U.S. policymakers of greater regulation of social media networks in EU and U.S. markets. It should be emphasized that implementation of these requirements will lead to greater public disclosure of social media companies. As part of these efforts, the EU and U.S. should also build on the CISA *Election Security Initiative* to create a transatlantic task force with a similar mandate. This can facilitate the sharing of best practices, which can help limit the spread of disinformation and protect elections in Ukraine and beyond.

- **Formulate and approve policy package focused on mandatory social media standards:** Through the TTC, a policy package for mandatory social media standards should be formulated. Measures should include requirements for removal instead of labeling disinformation, spending on anti-disinformation tools as a percentage of revenues, and provisions enabling the auditing of social media platforms' conduct through the European Commission and a dedicated U.S. government unit.
- **Lobby for internationalization of standards:** Recognizing the daunting challenge of disinformation in an age of political polarization, the policy package should be understood as a first step. Over time, the U.S. and the EU should lobby for the creation of international bodies fighting disinformation and regulating big tech at a global level. Conducive to this is engagement in existing forums such as the G20 and the UN.
- **Incentivize more detailed media coverage of Russian brutality:** Amid growing Ukraine fatigue, the EU and the U.S. should encourage media outlets to show greater graphic evidence of Russian crimes. On the EU side, the Commission should engage with media outlets through the *European Alliance of News Agencies* and the *European Federation of Journalists* to communicate its intentions of using graphic evidence as means to retain European support of Ukraine. At the member state level, the Commission should encourage EU representations to engage with media outlets domestically. In the U.S., policymakers should engage with the leadership from domestic news outlets representing the political spectrum such as the *Associated Press, Fox News, The New York Times, NPR,* or *USA Today*. Both the EU and the U.S. should also point to existing coverage of the brutality by promoting a list of resources on official government websites and on social media presences.

Recommendations: The Ukrainian government should support eastern Ukrainian media outlets known for producing quality content more actively by creating financial and political incentives that make spreading disinformation less attractive.

- **Create a fund for media infrastructure reconstruction:** As much of eastern Ukraine is destroyed, the Ukrainian government should create a dedicated fund for post-war reconstruction of media infrastructure. While this measure is of short-term political significance and cannot be meaningfully implemented until fighting stops, the government should also address immediate needs wherever possible. This includes supporting the work of civil society groups like the *National Union of Journalists of Ukraine*, which identified access to generators, power banks, computers, and other equipment alongside financial support for local journalists as most pressing. Since gaining access to the occupied regions remains difficult, whenever getting the equipment into the region is not possible, it should go to other news outlets with a track record of covering the Russian invasion truthfully.

- **Re-align financial and political incentives to disincentive spreading disinformation:** The Ukrainian government should embrace a carrots and sticks approach with regards to media groups. In the context of the war, this can mean creating financial incentives that reward those news outlets across Ukraine that established a reputation for reporting truthfully about civilian harm. It can also include the creation of a dedicated column-like showcase of outstanding news outlets that withstand the invasion by reporting fearlessly about Russian crimes. This column should become part of the social media content that politicians, governments in third party countries, and online influencers share.

- **Collaborate with the private sector to enforce disinformation standards:** As part of the sticks approach individuals, accounts, and organizations found to spread disinformation, should be sanctioned with immediate platform removal instead of just being labeled as spreaders of disinformation. Based on users' IP and email addresses, entities and individuals associated with disinformation should be banned from platforms for several months. To achieve cross-sector alignment, the Ukrainian government should leverage its ties with big tech and emphasize that disinformation, alongside Russian kinetic warfare, is a key obstacle to Ukrainian freedom. Considering that public opinion has proven to be effective in creating pressure for social media firms, this narrative should be accompanied by a public shaming campaign that refers to disinformation cases that created harm to the Ukrainian cause.

Cyber Operations

Tool 2: Dismantling Government and Private Organizational Software

From the days prior to the invasion up to today, the Ukrainian government finds itself under almost constant attack.[63] To weaken Ukrainian cyber defenses and government infrastructure for example, a Russian cyberattack was launched on January 13, 2022. As a result, 70 government websites were captured. In mid-February, another attack targeting government departments was launched. A final pre-war attack on February 23, 2022, targeted several ministry websites.[64] Since the beginning of the invasion, Russia continues to target the Ukrainian government. As of January 2023, a total of 500 cyberattacks against the government were recorded. An additional 300 attacks of a total of 2,000 Russian against Ukrainian entities targeted the security and defense sector, whereby many of the targets are directly or indirectly affiliated with the government.[65]

Since the beginning of the invasion, Russia continues to target the Ukrainian government. As of January 2023, a total of 500 cyberattacks against the government were recorded. An additional 300 attacks of a total of 2,000 Russian against Ukrainian entities targeted the security and defense sector.

Among the noteworthy examples of Russian cyberattacks against Ukrainian public entities is an attack launched in August 2022 against the country's nuclear energy agency. Widely regarded as the most ambitious effort against the organization, the attack had potential to disrupt the power grid and to disrupt oversight of 15 nuclear facilities. Although Ukrainian sources report that the attack failed to produce the attackers' desired results, it serves as a reminder of the potentially destructive impact

[63] Google (2023). Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape.

[64] Przetacznik, J., Tarpova, S. (2022). Briefing - Russia's war on Ukraine: Timeline of cyber-attacks. European Parliamentary Research Service.

[65] Miller, M. (2023, January 11). Russia's cyberattacks aim to "terrorize" Ukrainians.

cyberwarfare can have.[66] Another powerful example is a malware attack against the Ukrainian military's *Viasat* satellite communications system on the day of the outbreak of the war. As a result, communication within the military was hindered and civilians were denied access to information.[67]

In the private sector, almost all industries have been under attack. However, many organizations were able to move their data to cloud servers located outside of Ukraine, which prevented permanent data destruction. Regardless, cyberattacks continue to create challenges for many of the reported 21 sectors attacked in 2022.[68] Based on evidence from the *CyberPeace* Institute, the financial sector faces the brunt of attacks. Other sectors that are popular targets are transportation, trade, administrative and support sectors.[69]

Although it is difficult to compare attacks in their severity across sectors, some that stand out are a July 2022 attack against a large internet provider from which around 300GB of data was stolen, and the hack of an administrative center from which information of at least 227,220 people was taken. Following the first attack, more than 100 Ukrainian websites were manipulated and misrepresented. Following the second attack, malicious actors obtained information about Ukrainian citizens, among them civilians, which pro-Kremlin actors could use to attempt to break resistance by threatening individuals with personal consequences for non-subjugation.[70]

Among the tools of Russian cyber groups are phishing, wiper malware, and the use of software with replication capability that can spread malware across networks.[71] Russian groups are also using distributed denial-of-service attacks (DDOS), which enable attackers to overwhelm targets with fake traffic stemming from the utilization of multiple connected devices.[72] To date, DDOS attacks appear to be the most popular tool against Ukraine with a share of 87.3% of all reported cyberattacks

[66] Santora, M. (2022, August 16). The operator of Ukraine's nuclear plants says it faced an ambitious cyberattack.; Miller, M. (2023, January 15). Ukraine calls for "Cyber United Nations" amid Russian attacks.

[67] CyberPeace Institute (2022a). Case Study: Viasat.

[68] Amazon (2022, June 9). Safeguarding Ukraine's data to preserve its present and build its future.

[69] CyberPeace Institute (2023).

[70] CyberPeace Institute (2022b). Cyber Dimension of the Armed Conflict in Ukraine. *Quarterly Analysis Report Q3 from July to September 2022.*

[71] Microsoft (2022, June 22). Defending Ukraine: Early Lessons from the Cyber War.

[72] Coble, S. (2022, February 24). Ukraine Attacked with Wiper Malware.

as of late 2022.[73] On several occasions, organizations were targeted in the cyber and kinetic space simultaneously or in immediate sequence. Some examples for this strategy are coordinated cyberattacks against the Dnipro government agency and strikes against government buildings on March 11, 2022, or a destructive cyberattack against a Lviv-based logistics provider on April 19, 2022 and missile strikes against the company's transport network on May 3.[74]

Tool 3: Conducting Espionage and Collecting Military Intelligence

Since the outbreak of the war, espionage has become the focus of Russian cyberwarfare.[75] The underlying aim appears to be to gather information that can help weaken Ukraine and its battlefield position. Related efforts have been continuous.[76] Already prior to the war, various Russian government groups breached the cyber defenses of the Ukrainian military, diplomatic and humanitarian entities. All of these can possess important intelligence that could be helpful for the Russian military. Although a number of attempts were successful, it is hard to evaluate their overall effectiveness, especially with Ukrainian authorities keeping many of the attacks under wraps to prevent increasing Moscow's confidence.[77] It also remains unclear what kind of information could be collected and how the accessed data, if at all, influenced President Putin's decision making before the war.[78] What is evident amid the standoff on the battlefield is that Russian decisionmakers fail to meaningfully integrate the collected intelligence into their military planning. That does not mean that these attacks have not produced harm or that they cannot inflict detrimental repercussions on Ukraine in the medium-term.

Most Russian cyber espionage operations focus on countries supporting Ukraine. A June 2022 *Microsoft* study reported that a total of 128 organizations in 42 countries were targeted by pro-Kremlin cyber espionage. The aim of these attacks appears to be to obtain government information about the tenets of support of Ukraine. This interpretation appears consistent with the attackers' targeting strategy, which

[73] CyberPeace Institute (2023).

[74] Microsoft (2022, June 22).

[75] Bateman, J. (2022). Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences and Implications.; Murphy, M. (2022, December 21). Espionage, Not Blackouts, Is Theme of Russian Hacking in Ukraine.; Microsoft (2022, June 22).

[76] Murphy, M. (2022).

[77] Starks, T. (2023, February 16). What we've learned from a year of Russian cyberattacks in Ukraine.

[78] Bateman, J. (2022, December 16).

involves targeting government agencies in 49% of cases. Other strategic targets were think tanks providing foreign policy recommendations and critical defense companies in the energy and other economic sectors. So far, it is NATO countries that are at the center of Russian cyber activities outside of Ukraine with a staggering 63% of attacks targeting such countries. Among these countries, it is the U.S., Poland, Latvia, Lithuania, Denmark, Norway and NATO candidate countries Sweden and Finland that were attacked most. Out of the assessed attacks, 29% appear to have been successful.[79]

So far, it is NATO countries that are at the center of Russian cyber activities outside of Ukraine with a staggering 63% of attacks targeting such countries. Among these countries, it is the U.S., Poland, Latvia, Lithuania, Denmark, Norway and NATO candidate countries Sweden and Finland that were attacked most. Out of the assessed attacks, 29% appear to have been successful.

Since June 2022, attacks against NATO and EU members have likely only increased. That at least some of these attacks should be understood as means of retaliation against Western weapons support becomes evident when considering the case of attacks against Germany. Directly following the announcement of a politically sensitive, strategically important delivery of Leopard 2 tanks to Ukraine, several websites of the federal government, private companies, financial organizations, and airports were breached through DDOS attacks.[80] Beyond retaliation, the intention likely was to gain access to confidential information related to political and military considerations underlying the German decision to send these tanks.

Another example of cyberattacks against nations supporting Ukraine could be observed at NATO, which was the target of Russian cyber espionage attempts. By posing as representatives of the Portuguese NATO ambassador, Russian groups hoped to obtain confidential information through a phishing campaign, which was unsuccessful.[81] Similarly, there was a spying effort on an oil firm in an undisclosed NATO country in retaliation for the country's support of Ukraine.[82] By attacking this company, located in a country that still imports Russian oil, hackers likely tried to obtain knowledge about the rationale for continued imports, and potential phase-out

[79] Microsoft (2022, June 22).

[80] Euronews (2023, January 26). Russian hackers launch cyberattack on Germany in Leopard retaliation.

[81] Sky News (2022, July 19). Russian cyber spies targeting NATO countries in new hacking campaign.

[82] Lyngaas, S. (2022, December 20). Kremlin-linked hackers tried to spy on oil firm in NATO country, researchers say.

plans. Although knowledge about any of these would likely not enable Russia to advance its war efforts, it would provide context for blackmailing NATO importers in particularly energy insecure situations with Russian oil.

Tool 4: Damaging or Destroying Ukrainian Critical Infrastructure

Another element of Russian cyberwarfare includes targeting Ukrainian critical infrastructure. From February 24, 2022, until early April 2022, at least 40 cyberattacks with permanent destructive capability were carried out. 40% of these attacks targeted organizations operating in Ukraine's critical infrastructure sector.[83] Until today, cyberattacks against critical infrastructure, particularly through cyber fires, remain a constant feature of the war.[84] According to the *Ukrainian Computer Emergency Response Team*, more than 400 out of a total of 2,000 recorded cyberattacks in 2022 targeted entities in commercial, energy, financial, telecommunications, and software sectors - all of which deliver critical services to civilians. The aim of pro-Kremlin groups seems to be to break civilian resistance to the Russian invasion.[85] As with missile strikes on civilian targets like maternity wards, kindergartens, or shopping malls, the Russian government shows that it seemingly does not care about the potential loss of life as a result of cutoff from critical infrastructure like energy.

From February 24, 2022, until early April 2022, at least 40 cyberattacks with permanent destructive capability were carried out. 40% of these attacks targeted organizations operating in Ukraine's critical infrastructure sector.

Accordingly, Russia focused its military action during the first winter of the war on conducting what President Zelensky labels *energy terrorism*, both through kinetic and cyberwarfare. By bombing power supply outlets, President Putin's military cut off the energy supply of nearly 9 million Ukrainians as of December 2022.[86] While similar entities were targeted during the weeks leading up to the illegal annexation of Crimea, much of the energy supply was disrupted by Russian cyberattacks. To date, this has not been the case. However, Ukrainians should not hope that cyberattacks

[83] Microsoft (2022, April 27). Special Report: Ukraine - An overview of Russia's cyberattack activity in Ukraine.

[84] Bateman, J. (2022, December 16).

[85] Miller, M. (2023, January 11).

[86] Reuters (2022, December 26). Zelenskiy: power shortages persist, nearly 9 million Ukrainians without electricity.

won't deliver on the attackers' goals as attacks become more sophisticated and cyber tools adapt to cyber defenses.[87]

In fact, a multitude of cyberattacks against Ukraine's energy supply has been seen, although with limited impact, which was often overshadowed by kinetic attacks. For instance, in April 2022, several high-voltage electrical substations in Ukraine were attacked with malware. Although the attack did not cause power outages, the malware was able to move from the substations' IT network to its industrial control system before failing to surpass Ukrainian cyber defenses.[88] While cyber operations against industrial plants and critical infrastructure require preparation and planning, for which the Kremlin likely did not have the time in the early days of the war, they remain a threat. So far, it seems like Russia counts on creating a cumulatively destructive effect through many smaller cyberattacks.[89]

Two impacts are created by Russian cyber operations targeting critical infrastructure. As a first order effect, and due to a mix of kinetic and cyberwarfare, Ukrainians at times find themselves without access to critical services such as energy. This aggravates the devastating situation of the economy, and worsens the quality of life measured in terms of the average citizen's perception of safety. As a second order effect, cyber operations have at least partly been successful in instilling fear and supporting Kremlin propaganda. For the most part however, cyberattacks on critical infrastructure had "no perishable impact [...] to impeding or in any other way obstructing with the Ukrainians' ability to replenish and restore themselves."[90] One should not forget though that time to recover from such attacks can be detrimental to people's morale. This implies that the longer recovery takes and the more severe attacks become, the higher the toll measured in terms of psychological impact. Therefore, it will be crucial to build resiliency to prevent significant damage to critical infrastructure.

While some cyberattacks had massive impact potential, and others were very disruptive, they failed to achieve Russia's key aims: breaking morale, meaningfully weakening cyber infrastructure, and helping bring the country under Russian control. This is largely due to the Kremlin's inability to effectively break through

[87] Lyngaas, S. (2022, November 5). Russian missile strikes overshadow cyberattacks as Ukraine reels from blackouts.

[88] Canadian Centre for Cyber Security (2022, July 14). Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine.

[89] Lyngaas, S. (2022, November 5).

[90] Bateman, J. (2022, December 16).

Ukraine's cyber defenses, the Ukrainians' remarkable resilience in cyberspace as a result of years of building up capability in response to Russian attacks, and third party support. Third party's notable contributions include public-private partnerships to fend off attacks, support in moving data to the cloud to protect it from permanent damage, and hacktivist activity to counter Russian cyber aggression.

However, this should not lead one to believe that Russian aggression in cyberspace is not real. As the war lingers on and continues to represent a longer affair than initially estimated by President Putin, there is a real risk of escalation, also in cyberspace. Considering that cyberattacks keep Ukrainian organizations busy, there is also a significant opportunity cost associated with upholding defensive capabilities. Therefore, the attacks have an important impact, and fending them off will play a key role for the private and public sectors.[91]

Addressing Russian Cyber Operations

In fighting software breaches, espionage, and attacking critical infrastructure, Ukraine continues to benefit from effective support from big tech companies like *Amazon, Google,* or *Microsoft*. In combination with pre-existing domestic contingency plans, which are the result of an almost one decade-long struggle to fend off Russian cyberattacks, these companies help increase the resiliency of deterrence structures. Both factors combined contributed to a halving of cyberattack attempts from a recorded total of 290 separate attacks in February 2022 to around 140 monthly attacks by August 2022.[92] The resources big tech companies contribute include tech and monetary assistance,[93] government, industry relationships, and connections to Ukrainian cyber defenders,[94] cloud and European data center access,[95] alongside in-depth analyses of the cyber threat environment.[96] Particularly cloud access and the resulting availability of data backups has been key as it curtails Russian attackers' ability to cause permanent damage.

[91] McLaughlin, J. (2023, March 3). Russia bombards Ukraine with cyberattacks, but the impact appears limited

[92] Corfield, G. (2023, January 7). Russian cyberattacks on Ukraine halved with help from Amazon and Microsoft.

[93] Chang, E. (2022, July 5). Microsoft Shows Its Power Against Russia.

[94] Atkins, S. (2022, August 30). A web of partnerships: Ukraine, operational collaboration, and effective national defense in cyberspace.

[95] Bateman, J. (2022, December 16).

[96] Chang, E. (2022, July 5).

It is also *Starlink* systems, whose distribution is co-funded by *SpaceX* and several Western governments, that increase the security of Ukrainian telecoms.[97] Referred to by some experts as the most important digital war-time support, *Starlink* ensures reliable communication for front-line Ukrainian forces. The systems help support alignment between military command and on-the-ground operations. In doing so, they are particularly resilient to external disruptions.[98] However, the supply of *Starlink* satellites has not been without controversy. Despite being widely recognized as essential to Ukrainian military communications, the issuing company's CEO Elon Musk made clear that funding and further delivery of new *Starlink* systems is unlikely to continue in the long-term. Amid Musk's support of a controversial peace plan, which includes ceding Ukrainian territory to Russia,[99] and *SpaceX*'s efforts to prevent satellite use for drone control, it is unclear how conducive the systems are to Ukraine's cyber defense in the long-term.[100]

It is also improved end-point security systems based on the use of AI in big techs' cyber defense operations that have proven helpful. Through these technological advances, some of *Microsoft's* systems can recognize attack patterns early on and use that knowledge to stop malware from attacking further targets in much faster fashion than human-analysis can.[101] To better coordinate cyber defense domestically, Ukraine's cyber security agency has relied on sharing threat indicators and conducting joint training exercises with cyber defense experts across the country. Since these have proven to be important for the creation of a collective defense system, such approaches can provide an effective basis for future cyber defense efforts in Ukraine and beyond.[102]

From a transatlantic perspective, the European Commission and the U.S. government can do more to support the institutionalization of big tech support of countries under foreign attack in the context of a kinetic war. Since companies like *Microsoft* have only committed to providing their help at no cost until the end of 2023, and given that the conflict is likely to persist, securing cyber support in the long-term is pivotal to Ukraine's defense.[103] Moreover, the EU and the U.S.

[97] Metz, C. Vinograd, C., Cooper, H. (2022, October 14). Elon Musk Foments More Geopolitical Controversy With Ukraine Internet Dispute.

[98] Bateman, J. (2022, December 16).

[99] Metz et al. (2022, October 14).

[100] Roulette, J. (2023, February 9). SpaceX curbed Ukraine's use of Starlink internet for drones - company president.

[101] Bateman, J. (2022, December 16).

[102] Huber, N. (2022, November 8). What Ukraine's cyber defence tactics can teach other nations.

[103] Reuters (2022, November 3). Microsoft extends free tech support through 2023.

need to adapt better to Russia's use of gray zone tactics in cyberspace by practicing more pronounced deterrence and more effective campaigns for crisis response, both in case of war-related attacks on Ukraine but also on other countries. For cyber operations, resiliency and defense operations are critical. Therefore, the EU and U.S. must prioritize deeper intelligence sharing, particularly through new cybersecurity entities that are developed by the EU. Taken together, leveraging AI, feedback mechanisms, and open source intelligence can be important to outpace Russia's capabilities.

On the part of the Ukrainian government, immediate attention should focus on better coordinating pro-Ukrainian hacktivist groups. Recognizing that bolstering cyber defenses in the midst of war is a challenging endeavor, this is a low hanging fruit with great impact potential that can be immediately implemented. It appears that Ukrainian authorities have some oversight over some hacktivists groups, however there is no real control mechanism that Ukrainian officials can use to prevent hacktivists from overstepping lines that can escalate the conflict. While it is widely considered benign to have hacktivists support Ukrainian cyber defense, counter-attacks against Russia can stretch that understanding.[104]

It is unfeasible to think about creating a formal control mechanism, therefore, the Ukrainian government should use its public messaging on cyber hacktivism to emphasize the focus on deterrence and defense instead of on counter-attacks. Informed by the realization that cyberwarfare does not seem to make a big difference for the war's outcome, the *Security Service of Ukraine*, the country's Cyber-Security Agency, and the military's administrators should formally commit to asking for support of Ukraine's cyber defense - and only of that. Leading political officials should use their social media channels to underline that message. While this move might not fully deliver on the objective of re-gaining more control of hacktivists, it represents a credible attempt, which can shield the government from criticism that otherwise bolsters domestic EU and U.S. groups opposing continued support of Ukraine.

Starting now, the Ukrainian government also needs to actively encourage the buildup of in-house cyber defense mechanisms of targeted private and public sector organizations. Immediate steps that the government should take while the war lingers on include playing a more active role in institutionalizing the in-kind big tech support that it is receiving, both with the objective of ensuring resilience of Ukraine's cyber defense and of creating best practices for targeted governments in the future. As part of ensuring

[104] Waterman, S. (2023, February 21). Ukraine's Volunteer Cyber Army Could be Blueprint for the World: Experts.

the resilience of Ukraine's cyber defense, the Ukrainian government must think about alternative, more permanent sources of support beyond big tech contributions. Once violence and kinetic warfare recedes, the Ukrainian government should create and enforce mandatory requirements related to minimum levels of in-house cybersecurity protection of private and public entities operating in Ukraine.

In thinking about a post-war Ukraine, the Ukrainian government should focus on re-constructing an electricity grid that is less vulnerable to cyberattacks. This can help improve the resilience of critical infrastructure assets and reduce direct threats to the well-being of consumers, particularly in face of a kinetic conflict alongside attempts to destroy life-supporting infrastructure. Some strategies to achieve this objective could include a security-by-design approach, the utilization of advanced software solutions with development feedback cycles, and the application of best practices from similar projects like the U.S. Department of Energy's investment in next-generation cyber tools to protect American power supply. However, insights from projects like the latter need to be taken with the caveat of uncertainty about the extent of Chinese-made components in the grid.[105]

Recommendations: The European Commission and the U.S. State Department's Bureau of Cyberspace and Digital Policy should facilitate the creation of an international body that institutionalizes big tech cyber support for nations under adversarial attack. The EU and U.S. should also create a task force as the basis for deeper intelligence sharing between ENISA and CISA.

- **Facilitate the creation of an international body dedicated to "big tech" cyber support:** Given the important role that big tech support plays in Ukraine's self-defense in cyberspace, the European Commission and the *Bureau of Cyberspace and Digital Policy* should support Ukraine's efforts to create an international institution dedicated to big tech cyber support. Both actors should leverage their diplomatic relationships and use forums such as the G7, G20, NATO, and UN to work on building buy-in. Although the U.S. has traditionally blocked deeper international regulation of and cooperation on big tech, the war in Ukraine creates unique momentum for the European Commission to change the U.S.'s stance. By reference to American big techs' cybersecurity contributions to Ukraine's self defense and

[105] U.S. Department of Energy (2022, August 17). DOE Announces $45 Million for Next-Generation Cyber Tools to Protect the Power Grid.

the prospect of post-war business opportunities, the Commission should frame participation in an international institution as conducive to creating American jobs, tax incentives, and other economic benefits; all of which would benefit American companies' international competitive position. The U.S. State Department's *Bureau of Cyberspace and Digital Policy* should work closely with private sector companies based in the U.S. who have supported previous information-sharing efforts. These efforts should also be supported by State's *Bureau of International Organizations*.

- **Create a task force for deeper ENISA-CISA intelligence sharing:** The transatlantic effort to counter Russia's gray zone tactics should aim to outpace Russia's intelligence capabilities through strategic coordination. Such coordination should happen on artificial intelligence, where experts across the EU and U.S. government agencies should work together on finding meaningful ways to understand attack patterns with AI. This will expand data sets, which can help expand AI capabilities and thus increase success of existing tools. With the aim of creating a mandate for greater ENISA-CISA intelligence sharing, a EU-U.S. task force should be set up to discuss conditions for such an arrangement. The task force should be created with explicit support of the highest levels of EU and U.S. authority. It should bring together transatlantic intelligence experts, policymakers, and cybersecurity specialists and aim for a deepening of intelligence sharing on cyber by early 2024. Closer cyber coordination has previously failed due to lack of institutional development on the European side as a result of underestimation of the challenge. Official intelligence sharing channels on cyber also remain absent between NATO and the EU due to differing transatlantic approaches to private information and cloud computing.[106] This has over the years created a lack of trust, which long disincentivized attempts to achieve progress on cyber coordination. Therefore, harmonizing standards with regards to these two issues has to be a key focus area of the task force. With increasing cyber institutionalization on the European side, and reinforcement of value-based transatlantic unity in response to Russia's invasion of Ukraine, the time is right for the task force to achieve meaningful progress.

[106] Kolmos, C. (2021, February 24). Bridging the Transatlantic Cyber Rift: Recommendations for Cyber Cooperation Between NATO and the EU.

Recommendations: The Ukrainian government should focus immediate action on better coordinating hacktivist groups and emphasize that it rejects counter-attacks on Russia. To ensure continued resilience of cyber defenses in the war, the government should take steps to institutionalize big tech support and lead an international movement for the creation of an international organization that ensures in-kind defenses for governments under adversarial attack. It should also begin encouraging the further build-up of in-house cyber defenses of private and public entities in Ukraine.

- **Increase active engagement with pro-Ukrainian hacktivist groups:** The Ukrainian government should position itself as being in favor of cyber defense but not of counter-attacks. Recognizing that such attacks could provide arguments to foreign groups critical of the economic costs of their respective country's continued support of Ukraine, the government should use its existing lines of communication with hacktivist groups to communicate their rejection of counter-attacks. Government officials like President Zelensky should also use their public messaging to openly communicate their opposition to cyber maneuvers that go beyond directly defending Ukraine. While likely not fully effective in terms of shifting behavior of all groups, these attempts can shield the government from credible criticism by EU and U.S. domestic fractions opposed to further support.
- **Institutionalize big tech support for Ukraine's cyber defense:** The Ukrainian government should initiate and lead the campaign aimed at the creation of an international organization with a cyber mandate. This organization should encompass support from big tech, which commits to provide cyber aid to struggling nations under cyberattack. The Ukrainian government should build on nascent efforts to call for the creation of a UN-like cyber entity and on the classification of cyberwarfare as war crimes.[107] Ukraine should emphasize the pressure that cyberwarfare poses in the war. It should bring up opportunity costs that come with continuously having to strengthen cyber defenses while physically defending the country. Relations with big tech should be leveraged, and the organization should be framed as an opportunity for big tech to be perceived as corporate citizens. However, reliance

[107] van Sant, S. (2023, January 9). Kyiv argues Russian cyberattacks could be war crimes.

on corporate goodwill is insufficient. To create conditions that make big tech companies likely to participate in such an organization, business incentives need to be created. These include the prospect of for-profit contracts after in-kind support, and tax benefits for future operations. During Ukrainian reconstruction, such contracts and benefits should be given out preferentially to big tech companies that supported the country during the war. The case should be used to recruit big tech support for an international organization that institutionalizes big tech cyber support alongside follow-up business incentives.

- **Take initial steps to incentivize domestic entities to build up in-house cyber defenses:** The Ukrainian government should lead by example and publish information about the far-reaching efforts of public agencies to meet the cyber threat. This should include greater disclosure about near misses that the authorities could fend off due to the strength of domestic and international efforts to shield Ukrainian cyber infrastructure. Such disclosure could happen through monthly reports. Through this level of transparency, the cyber threat can be spotlighted, which can increase risk perception of private entities and contribute to a renewed commitment to improving existing in-house structures. In being transparent, it is important to strike a balance between encouraging other organizations to model cyber defense efforts and not increasing vulnerability to enemy attacks. Therefore, disclosures should be general instead of technical and feature data such as number of averted attacks, or overall financial investment in cyber defense.

Recommendations: In the long-term, the Ukrainian government should build on its efforts to encourage the creation of in-house cyber defenses by supplementing them with policies that mandate minimum cybersecurity standards for Ukrainian public and private entities. In thinking about post-war Ukraine, the government should focus on re-constructing an electricity grid that is less vulnerable to cyberattacks.

- **Mandate strengthening in-house cyber defenses for Ukrainian public entities through policy:** To build on efforts to strengthen in-house cyber defenses during the war, the Ukrainian government should mandate compliance with a set of minimum cybersecurity standards that all public and private entities above a certain size have to fulfill. These standards should be grounded in research and expert insights on which measures worked well in fending off Russian cyberwarfare. They should be the result of a working group's cross-sector consultations and input from big tech companies that supported Ukraine's cyber defense. Compliance with these standards should be mandated through national policy. To reduce the risk of non-enforcement, the policy should be supplemented with complimentary access to public resources that broadly follow the model of CISA's catalog of free public and private sector cybersecurity resources.

- **Prioritize a "security-by-design" approach in post-war reconstruction:** After the war, the Ukrainian government should prioritize cybersecure reconstruction, especially in critical infrastructure. To ensure that all aspects of infrastructure reconstruction address the aim of increasing the country's cybersecurity, the government should pass a law that mandates a detailed cyber threat assessment and concrete measures to address these threats for all critical infrastructure projects in the country. Project approval from the government should be made conditional on compliance with this law, both nationally, and regionally. The government should provide guidelines according to which infrastructure projects are to be set up for built-in cyber defenses, especially in the during the war particularly targeted energy sector. These guidelines should be the result of consultations with big tech partners, which wherever appropriate should be chosen as project partners based on a comparative assessment of the capabilities concerning a specific infrastructure sector's cyber protection.

Policy Challenge 2: Defending the Transatlantic Partners against the Chinese Cyberwarfare Threat

According to the 2022 U.S. *National Security Strategy*, Russia continues to pose an immediate short- and medium-term threat to the U.S. and EU. However, China poses more of a long-term strategic threat to security and stability in cyberspace. This dynamic was aptly described by National Security Agency Cyber Director Rob Joyce, who perceives "Russia as the hurricane [that] comes in fast and hard", while China resembles "climate change [that represents a] long, slow, pervasive [threat]."[108] This captures Russia's use of cyberattacks to cause sudden and unpredictable damage, in comparison to the People's Republic of China's (PRC) focus on slowly building strategic cyber capabilities, like digital data theft and offensive cyberattacks, as mechanisms for reaching global superpower status. Therefore, any discussion of addressing the global cyberwarfare challenge would be incomplete without reference to China's cyber capabilities and the strategic challenge they pose to U.S. great power status and Western international leadership.

> This dynamic was aptly described by National Security Agency Cyber Director Rob Joyce, who perceives "Russia as the hurricane [that] comes in fast and hard", while China resembles "climate change [that represents a] long, slow, pervasive [threat]."

Even with Russia's ongoing cyberattacks in Ukraine, it is critical that the partners do not lose sight of the longer-term strategic threat posed by China's cyber capabilities. The transatlantic partners simply cannot afford to be entirely distracted by Russia's belligerent actions, while China develops advanced cyber capabilities unchecked. China's actions in cyberspace hurt the development of democratic norms and prevent an open and free internet that the EU and U.S. have long fought for. These efforts run counter to more collaborative interactions with China in other policy realms such as addressing the threats arising from climate change. In this context, leveraging transatlantic partnerships is critical to counter such threats through joint preparedness, the build-up of response capability, and cost imposition on actors who violate cyber norms. Given the rapidly evolving threat landscape, deeper coordination, and closer policy alignment to protect the U.S., EU, and cyberspace is desirable.

[108] Langenkamp, A. (2022, May 8). From Russian rain to Chinese storm.

However, implementing and maintaining a long-term strategic transatlantic partnership to address China's activity in cyberspace remains a significant challenge given the evolving threat environment, differing approaches to data privacy, and nuanced diplomatic relationships between the U.S., EU, and China. There is transatlantic tension about how severe the threats posed by China are, and the EU leans more towards embracing cooperation, over competition; particularly in economic partnerships and international trade. For example, China overtook the U.S. as the EU's largest trading partner in 2020.[109] Trade between the EU and China reached nearly €850 billion in 2022 and represents €2.3 billion daily in 2023.[110] As a result of this more deeply intertwined trading and economic relationship, the EU practices a more collaborative, and at times, peer-like approach to China. EU leadership has been hesitant to take the same combative approach that U.S. policymakers have embraced over the last five years. Given this dynamic, it is critical that the U.S. and EU find ways to institutionalize coordination on shared priorities that acknowledge the tensions, but also economic dependencies, of both the EU and U.S. relationship with China.

Trade between the EU and China reached nearly €850 billion in 2022 and represents €2.3 billion daily in 2023. As a result of this more deeply intertwined trading and economic relationship, the EU practices a more collaborative, and at times, peer-like approach to China.

Ultimately, the EU and the U.S. grapple with an ever-changing cyber threat landscape that targets democratic values and weakens the security of cyberspace. The myriad of geopolitical challenges and threats to democracy, ranging from Russia's invasion of Ukraine to China's disregard for cyber norms, present a strong imperative for transatlantic cooperation and norm establishment on cyber defense. If the U.S. and the EU do not take concerted action to build stronger coalitions for international norms and to overcome past differences, authoritarian powers like Russia and China will seek to proliferate offensive cyber capabilities and reshape the international order through the establishment of authoritarian-inspired cyber norms.

[109] BBC News (2021, February 17). China overtakes US as EU's biggest trading partner.

[110] European Union External Action Service (2023, April 13). My view: China and EU-China relations.

The Primary Strategic Threat: The PRC's Actions in Cyberspace

As outlined in the new U.S. *National Cybersecurity Strategy*, the PRC "presents the broadest, more active, and most persistent threat to both government and private sector networks".[111] From a transatlantic allied perspective, China's embrace of cyber tools for malicious purposes poses a significant and long-term threat to secure and stable cyberspace. Furthermore, the PRC's actions in cyberspace run counter to shared transatlantic international objectives and showcase the critical importance of building a long-term transatlantic approach to cybersecurity partnerships.

The PRC's actions in cyberspace, including offensive cyber capabilities and espionage, cause economic and security damage to the U.S. and EU. In February 2023, ENISA and the *Computer Emergency Response Team of the European Union* (CERT-EU) alerted the international community that several Chinese military hacking groups (including APT27, APT30, APT31, Ke3chang, GALLIUM, and Mustang Panda) have stepped up targeting of EU businesses and organizations.[112] Recent operations focused on information theft through establishing persistent footholds within network infrastructures, and they used content on Russia's invasion of Ukraine for phishing lures targeting EU organizations.[113] In the U.S., Chinese state-backed hacker group APT41, described by researchers as "a prolific Chinese state-sponsored cyber threat group," compromised the computer networks of at least six U.S. state governments between May 2021 and February 2022.[114] In 2020, the U.S. Department of Justice indicted five Chinese nationals (some were part of APT41), with computer intrusion campaigns that affected over 100 companies in the U.S. and abroad.[115] The threat is only growing in sophistication. *Google's* Mandiant division recently found that Chinese state-sponsored hackers have developed more advanced techniques that thwart common cybersecurity tools that allow them to embed and spy on government and business networks for years without detection.[116]

[111] The White House (2023, March 1).

[112] ENISA, CERT-EU. (2023, February 15). Sustained Activity by specific threat actors.

[113] Greig, J. (2023, February 17). Multiple Chinese APTs are attacking European targets, EU cyber agency warns.

[114] Kharpal, A. (2022, March 9). China state-backed hackers compromised networks of at least 6 U.S. state governments, research finds.

[115] U.S. Department of Justice (2020, September 16). Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally.

[116] McMillan, R., Volz, D. (2023, March 16). Wave of Stealthy China Cyberattacks Hits U.S., Private Networks, Google says.

These are only a few, but clear, examples of Chinese APTs attacking both U.S. and EU targets. As a result of these continuous and growing shared threats, the EU and U.S. have committed to building "a resilient cybersecurity partnership; an open, interoperable, secure, and reliable internet; and stability in cyberspace."[117] Even with these malicious actions, effectively addressing strategic threats to the U.S. and the EU are complicated by differing relationships with China. Ramping up during the Trump administration and continuing into the Biden administration, the U.S. labeled China a strategic competitor and placed more severe trade restrictions and export controls with Chinese entities to counter China's influence. By contrast, the EU-China relationship has only recently begun to deteriorate, with tensions rising from China's counter-measures to EU sanctions on human rights, economic coercion against the EU's single market, and China's position on the war in Ukraine.[118] Even with these new geopolitical dynamics, the EU has not changed its view of China as "simultaneously a partner for cooperation and negotiation, an economic competitor and a systemic rival".[119] This strategic outlook was endorsed by the European Council in 2020 and has guided the EU's approach to China. Conversely, the U.S. has made a far more assertive commitment to "out-compete" China.[120]

Despite the complex relationships between China, the U.S. and EU, China's actions in cyberspace fundamentally threaten global democratic norms and the open internet, which is foundational to the transatlantic partners' democratic and secure vision for cyberspace. Through closer partnerships, the EU and the U.S. can address the three most significant threats posed by China's actions in cyberspace: 1) advanced offensive cyber capabilities, 2) economic espionage against both U.S. and EU businesses, and 3) the weakening of democratic governance norms in cyberspace.

Through closer partnerships, the EU and the U.S. can address the three most significant threats posed by China's actions in cyberspace: 1) advanced offensive cyber capabilities, 2) economic espionage against both U.S. and EU businesses, and 3) the weakening of democratic governance norms in cyberspace.

[117] U.S. Department of State (2022, December 21). 2022 U.S.-EU Cyber Dialogue Media Note.

[118] European Union External Action Service (2023, April 13).

[119] European Commission (2019, March 12). EU-China strategic outlook: A joint contribution by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Council.

[120] The White House (2022, October 12). National Security Strategy.

China's Advanced Offensive Cyber Capabilities

China is a major peer adversary to the U.S. in cyberspace. The country possesses offensive cyber capabilities that rival those of the transatlantic partners. The U.S. intelligence community warns that China "possesses substantial cyberattack capabilities [and] can launch cyberattacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States."[121] Additionally, in its use of its asymmetric capabilities, China is not constrained by international norms or domestic law like the U.S. and the EU are. China's "civil-military fusion" also boosted the nation's cyber capabilities and its ability to leverage vulnerabilities reported through Chinese private sector companies.

China's investments in cyber capabilities, and commitment to civil-military fusion are paying off. In fact, Beijing exploited six times as many zero-day vulnerabilities in 2021 as in 2020.[122] In November 2022, *Microsoft* accused Chinese state-backed hackers of abusing the PRC's stricter vulnerability disclosure requirements to develop these valuable, zero-day exploits. The rules that took effect in September 2021 were described by *Microsoft* as "a first in the world for a government to require the reporting of vulnerabilities into a government authority for review prior to the vulnerability being shared with the product or service owner." China used these capabilities to conduct global hacking campaigns, with Chinese-based groups targeting entities in Afghanistan, Kazakhstan, Mauritius, Namibia, and Trinidad and Tobago - in line with *China's Digital Belt and Road Initiative strategy*.[123]

In February 2022, *Symantec's* Threat Hunter team reported the discovery of a new malware called Backdoor, which was described as "exhibit[ing] technical complexity previously unseen by such actors."[124] This specific type of malware was used in a long-running espionage campaign against targets of strategic interest to the Chinese government, and it presents another example of China's advanced offensive cyber capabilities. Specifically, Chinese state and state-affiliated threat actors pursue government, diplomatic, and NGO sector targets to garner critical insights to drive Chinese economic espionage or traditional intelligence collection and national

[121] U.S. Office of the Director of National Intelligence (2021, April 9). Annual Threat Assessment of the US Intelligence Community.

[122] CrowdStrike (2023). 2023 Global Threat Report.

[123] Microsoft (2022, November 4). Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression.

[124] Symantec (2022, February 28). Daxin: Stealthy Backdoor Designed for Attacks Against Hardened Networks.

security objectives. [125] These advanced offensive cyber capabilities already impose considerable costs on target countries across the EU and in the U.S., but their costs and damages will likely only grow as Beijing develops its capabilities without restrictions imposed by a regulator or an international body.

Furthermore, the U.S. intelligence community alleges that the Chinese government is supporting the Russian cyberwarfare campaign that is targeting Ukraine's Western supporters. Given the Chinese government's stated commitment to reunite Taiwan with mainland China, under the long-proclaimed *One China Policy*, it will be important for the transatlantic partnership to prepare for a similar cyberwarfare campaign against a like-minded democratic system in the region. Since Taiwan has long been used as a test case for improving the effectiveness of Chinese cyberattack capability, the likelihood that cyber will play a role in a future cross-Strait conflict is high.[126] Therefore, any transatlantic effort to prevent cyberwarfare from becoming an effective war tool of adversaries in the future needs to address the further progression of China's advanced cyber capabilities and how to counter this dangerous evolution.

Furthermore, deeper coordination between the transatlantic partners must include more cohesive information and threat sharing. The EU and U.S. can save resources by jointly implementing critical infrastructure cybersecurity protection or increasing coordination on open-source threat analysis. Given how many cyberattacks hit companies that operate in the EU and U.S. markets, information sharing is critical for getting ahead of threats, and creating more rapid and coordinated responses.

Recommendations: Increase EU and U.S. Cyber defensive cyber capabilities and workforce development through strategic coordination and deeper institutional connectivity.

- **Establish transatlantic cyber liaison roles:** Set up liaison officers at the Department of Homeland Security, CISA, as well as the European External Action Service (EEAS) and ENISA. These liaison officers will own the transatlantic coordination portfolio and be responsible for identifying opportunities for coordination and to raise concerns to senior leadership at both agencies in case there are areas of tension.

[125] Microsoft (2022, November 4).

[126] Hsu, P. (2018, January 23). Chinese Hacking Against Taiwan: A Blessing for the United States?

- **Personnel and cyber workforce exchanges:** Establish a new EU-U.S. cyber fellowship to enable EU and US staff to intensify exchanges and strengthen trust and understanding in cybersecurity.

    - The EU-U.S. cyber fellowship would include hands-on experiences and cyberattack simulations to prepare the U.S. and EU workforce to more effectively coordinate in the event of a significant and global cyberattack like *NotPetya*.

    - The fellowship will be a critical networking building entity, and should include an annual summit or meeting for previous and current cohorts to connect and engage.

- **Align critical infrastructure cybersecurity standards and best practices through the U.S.-EU TTC:** The U.S.-EU TTC is an important vehicle for harmonizing transatlantic critical infrastructure cybersecurity standards. As an entity that was founded with the core mission of strengthening transatlantic relations, the TTC is a natural vehicle for institutionalizing transatlantic cyber coordination for critical infrastructure. Alignment efforts should include:

    - Both the EU and U.S. name a cybersecurity official from CISA, ENISA to be a representative at each TTC working group (for example, the Department of Commerce TTC line of effort).

    - Launch a TTC working group to focus on establishing tight coordination and reporting links with CISA and ENISA on securing critical infrastructure from cyberattacks.

    - Establish forums for private sector entities to partner with the Council by creating iterative engagement formats that focus on non-governmental contributions to cyber defense, which are portrayed as being in the shared interest due to implications for social cohesion, risk management, and safeguarding of economic assets.

Economic Impacts of China’s Malicious Action in Cyberspace

The Chinese Ministry of State Security’s economic-driven cyber espionage represents another significant threat for the U.S. and the EU. China engages extensively in efforts to acquire technology, which can potentially give the country access to sensitive trade and proprietary information through cyberattacks. Access to EU and U.S. technology can also weaken transatlantic innovation and economic competitiveness in the long-term. China is estimated to be responsible for 50 to 80% of cross-border intellectual property theft worldwide, and over 90% of cyber-enabled economic espionage in the United States alone.[127] The estimated cost to the U.S. economy resulting from this activity is estimated to be between $300 billion and $600 billion annually.[128] Considering the potential harm to competitiveness, the espionage attacks are likely aimed at helping support China’s relative competitive and economic position, thus helping advance its foreign policy objectives, and providing intelligence about adversaries.

China is estimated to be responsible for 50 to 80% of cross-border intellectual property theft worldwide, and over 90% of cyber-enabled economic espionage in the United States alone. The estimated cost to the U.S. economy resulting from this activity is estimated to be between $300 billion and $600 billion annually.

Increasingly recognized by ENISA as also posing a risk to the European business community and EU institutions, Chinese cyberattacks and IP theft require coordinated and strong transatlantic responses.[129] The imperative for such coordination only becomes stronger when considering the potential compounding impacts of adversarial cyberattacks resulting from the closely linked nature of the EU and U.S. economies. To date, the fragmented nature of cybersecurity standards in the transatlantic area inhibits coordinated responses and security. While it is not possible to completely align standards, the EU and U.S. should work more closely on defining economic espionage and creating a coordinated response to secure intellectual property and protect transatlantic economies.

[127] Blair, D.C., Huntsman, J. M. (2013). The Report of the Commission on the Theft of American Intellectual Property.

[128] Federal Bureau of Investigation (2019). Executive Summary - China: The Risk to Corporate America.

[129] CERT-EU, ENISA (2023, February 15). JP-23-01 - Sustained activity by specific threat actors.

Public-private partnerships are imperative to comprehensively tackle the ever-evolving threat posed by cybercrime and China's economic cyber espionage. Transatlantic private and government entities must establish trusted relationships for the real-time, two-way sharing of threat information to be effective. Cybersecurity entities in the U.S. and EU should more actively facilitate connections between multinational companies that have more robust cybersecurity capabilities to share best practices with companies across transatlantic markets. Workforce development in both the public and private sectors is another critical component of public-private partnerships and can help protect transatlantic economies from cyber-enabled economic espionage. The EU and U.S. governments (at both federal and local levels) need to increase funding for basic cybersecurity education and awareness, starting in secondary education. Additionally, substantial investments in higher education programs in cybersecurity and upskilling programs are essential for meeting the growing demand for cybersecurity professionals.

Although the most recent EU-U.S. Dialogues addressed coordinated responses to resiliency, there was no explicit mention of workforce development. Given the deep connectivity between the transatlantic economies, the EU and U.S. must begin working closely together on workforce development to address the impacts of China's cyber activity on EU and U.S. economies.

Recommendations: Strengthen transatlantic public-private partnerships and private sector engagement in U.S. and EU cybersecurity efforts:

- **Institutionalize public-private partnerships and collaboration during conflict:** Building on the historical engagement of the private sector before and during the Ukraine War, the U.S. and EU should create a body that facilitates constant and close coordination between major technology companies and private cybersecurity firms to communicate threats, patch vulnerabilities, and respond rapidly to cyberattacks. Similar to sector-specific ISACs, this new entity would bring together U.S. and EU companies and key cybersecurity agencies to identify and respond to cyber threats in a coordinated and streamlined manner. While this effort should begin with the U.S. and EU, it can be expanded to include cybersecurity organizations from other allies and partners.

- **Facilitate transatlantic information sharing and analysis centers (ISACs) coordination:** The TTC can invite EU ISACs and the U.S. *National Council of ISACs* for a series of roundtable discussions to propose solutions for stronger information sharing with private sector partners on transatlantic cyber threats. The roundtable should be tasked with providing clear recommendations at the end of the series.

- **Prioritize transatlantic-specific information sharing in the private sector:** Strengthen open-source analysis of threats and vulnerabilities that target companies in the EU and U.S. markets. The *EU Joint Cyber Unit* should include an initiative that focuses on working with ENISA and CISA to identify multinational companies with a larger market share and critical infrastructure that would impact the transatlantic economy for prioritized threat sharing.

- **Joint U.S. and EU commitments on coordinated responses to Chinese cyber espionage:** The EU and U.S. should make a public commitment to large-scale, coordinated attribution with countries that are impacted by Chinese commercial cyber theft and that the EU and U.S. will coordinate on concrete and targeted sanctions on organizations and individuals caught using cyberattacks to steal EU and U.S. intellectual property. CISA's *Joint Cyber Defense Collaborative* and the *EU's Joint Cyber Unit* should launch a partnership dedicated to coordinating intelligence sharing, threat identification, and attribution for cyber espionage.

China's Threat to Responsible and Democratic Norms in Cyberspace

If the U.S. and the EU fail to take decisive action to build broader coalitions and institutionalize democratic norms in cyberspace, authoritarian governments like the PRC can leverage their economic power and cyber capabilities to shape norms on their own terms. This is particularly concerning as many of the norms in cyberspace are still developing, and international alignment is needed for their institutionalization. However, China's irresponsible behavior in cyberspace also poses significant risk to maintaining some of the limited norms in cyberspace that exist.[130] China's emergence as a peer competitor in cyberspace and its growing

[130] U.S.-China Economic and Security Review Commission (2022, February 17). China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States.

presence in global standard-setting bodies showcases the urgency of EU-U.S. coordination to counter China's influence.[131]

China declared its intentions of becoming a "cyber superpower" and highlighted its goal to shape the establishment of global internet governance and standards, which is inherently related to that objective.[132] To achieve this goal, Beijing focuses on building influence in multilateral bodies with technology-related mandates to promote the technical foundations of its market share, cyber sovereignty, and the Digital Silk Road (DSR). As part of this approach, China aims to use existing vacuums in cyberspace to mainstream its understanding of which standards should govern international cyberspace. China views internet infrastructure standards as central to its own digital foreign policy. As a result, China's takeover of leadership positions in international technical standard-setting bodies has become a strategic foreign policy priority. These actions support President Xi's declaration that leading and setting internet governance norms is key to making China a great power in cyberspace.[133]

China also seeks to create new bodies to shape technology standards that help expand China's global influence. In this context, it is the concept of cyber sovereignty that represents the cornerstone of China's internet norms. According to China's 2017 *International Strategy of Cooperation on Cyberspace*, the principle of sovereignty means that "countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing."[134] Although this understanding might sound consistent with the international principle of self-determination, it implies a Chinese rejection of Western-inspired governance standards in cyberspace. This divergent approach will continue to increase tensions between democratic allies and China in the long run. It has the potential to undermine Western efforts to maintain the open internet, alongside the safety of critical infrastructure assets and intellectual property.

[131] Chinese Ministry of Foreign Affairs & Cyberspace Administration of China (2017). International Strategy of Cooperation on Cyberspace.

[132] U.S.-China Economic and Security Review Commission (2022). 2022 Annual Report to Congress.

[133] Xinhuanet (2015, December 16). Speech by Xi Jinping at the Opening Ceremony of the Second World Internet Conference (full text).

[134] Chinese Ministry of Foreign Affairs & Cyberspace Administration of China (2017).

For smaller, less economically affluent countries that are looking for cheaper digital products and services or that wish to push back on U.S. hegemony, China's *cyber sovereignty narrative* can be compelling. China leverages the DSR as a norms-promoting vehicle, also supported through various international projects of the Belt and Road Initiative that are based on cyber sovereignty as a guiding principle. As a result, China's approach to cyber governance has proven to be attractive to several developing countries that prefer the internet to be governed based on non-Western values. For example, Zimbabwe, Djibouti, and Uganda have explicitly indicated concerns over joining an internet that they believe to be "just a gateway" for digital colonization from Western internet companies.[135]

Through the DSR, China provides digital infrastructure and software at competitive prices, with little to no obvious strings attached. This runs counter to many developing countries' perceived Western insistence on neoliberal governance standards, which is usually associated with EU or U.S. infrastructure investments. The Chinese approach is gaining traction – as of 2019, China signed cooperative agreements with sixteen countries under the DSR framework.[136] DSR represents a significant tool in China's efforts to become a "cyber superpower", and Western nations need to recognize the urgency of providing a compelling alternative to China's version of the internet before it is too late.

The EU and U.S. can push back on this trend by identifying which existing digital standards threaten democratic and Western strategic interests most and by leveraging public-private partnerships to develop and implement new standards to address these challenges.[137] The robust transatlantic innovation and economic ecosystem is one of the greatest areas of strength to leverage in combating China's growing normative influence. Additionally, coordination on the international stage to leverage the combined economic and geopolitical influence of the EU and U.S. is critical for effectively shaping the global cyber agenda and the cybersecurity rules and policy responses by other countries.

China does not have the breadth of alliances and integration in the international community that the EU and the U.S. have together. However, the EU and U.S. can build more extensive alliances and agreements to promote an open, stable internet

[135] Adee, S. (2019, May 14). The global internet is disintegrating. What comes next?

[136] Xinhuanet (2019, April 22). Co-construction of the "Belt and Road Initiative": Progress, Contributions and Prospects.

[137] Faaborg-Andersen, S., Temes, L. (2022). The Geopolitics of Digital Standards.

and cyberspace. Conversely, the transatlantic partners must also coordinate when imposing economic or diplomatic costs on nation-states restricting access to information and the internet. Surely, the way the internet and social media are set up does not just incentivize the spreading of truthful information. The open internet also provides fertile soil for spreading disinformation and hatred. Therefore, further progress needs to be made on passing and enforcing internet governance standards. However, leaving internet governance to authoritarian powers like China is likely to restrict it in novel ways that stand in conflict with Western liberal conceptions. In this context, sanctions for states that seek to repress freedoms and human rights through restricting internet access will be more impactful than unilateral action.

China's Enabling of the DPRK's Destructive Cyber Behavior

The North Korean government's malicious activity in cyberspace has grown in sophistication. North Korea (DPRK) is increasingly enabling the disruption of international cyber and economic security. As the DPRK works through disaggregated criminal enterprises to support its nuclear ambitions through ransomware, stealing cryptocurrency, and other deployments of harmful IT, it represents a significant challenge to the transatlantic partners. According to the Biden administration's Deputy National Security Adviser for Cyber and Emerging Technology Anne Neuberger, North Korea "use[s] cyber to gain [..] up to a third of [stolen crypto] funds to fund their missile program." This appears consistent with a UN Report that estimates that between 2020 and 2021, North Korean-backed hackers stole more than $50 million in digital assets to fund the country's missile program. In 2019, the figure stood at $2 billion, all of which went towards the DPRK's nuclear program. Among the targets were at least three cryptocurrency exchanges in North America, Europe, and Asia.[138]

Between 2020 and 2021, North Korean-backed hackers stole more than $50 million in digital assets to fund the country's missile program. In 2019, the figure stood at $2 billion, all of which went towards the DPRK's nuclear program.

The Lazarus Group, which is linked to the North Korean government, provides an example of a destabilizing force in cyberspace that has a significant impact

[138] BBC News (2022, February 6). North Korea: missile programme funded through stolen crypto, UN report says.

globally. This North Korean-sponsored hacker group is sanctioned by the U.S. Treasury Department for targeting critical infrastructure with cyberattacks. The group is considered responsible for stealing about $620 million in cryptocurrency in a hack of the virtual game *Axie Infinity*.[139] Furthermore, cybersecurity firms and research groups have attributed attacks on European defense contractors to Lazarus sub-groups.[140] Most notably, the U.S. and UK governments attributed the *WannaCry* malware attack in 2017 to the Lazarus Group. Described by Europol as an attack of "unprecedented scale," *WannaCry* affected hospitals, businesses, and banks in more than 150 countries. The malware caused billions in damages.[141]

Many North Korean hacker groups operate out of Russia and China, which makes attribution challenging. As evidence shows that cyber criminality provides a key facet of maintaining the DPRK nuclear program's viability, North Korea's cyber capabilities present a significant risk for destabilization of the Korean Peninsula and broader Indo-Pacific stability. North Korea seeks to exercise influence over both South Korea and its Western allies through cyber provocations, which poses a risk of escalation to kinetic engagement or possible use of WMDs in a worst-case scenario.

China allows for North Korean hacker groups to operate within their borders, which enables the destabilization of cyberspace. According to some estimates from 2016, around 600 to 1,000 North Korean cyberwarfare operatives conducted their activities from Chinese territory. Since then, this figure has likely only increased. Beyond that, most of the very limited North Korean internet traffic, among that cyberattacks, runs through Chinese internet access providers.[142] Considering the tight grip the Chinese Communist Party has on economic activities and people movement in its country, it is highly unlikely that North Korean cyber activity is being tolerated without high-level political support. Insofar, China is not just an enabler of North Korean cyberwarfare, but also an active ally in its perpetuation.

According to some estimates from 2016, around 600 to 1,000 North Korean cyberwarfare operatives conducted their activities from Chinese territory.

[139] Dress, B. (2022, April 15). North Korean group stole more than $600M in Axie Infinity hack, FBI says.

[140] ESET (2022, June 1). ESET Research: Lazarus attacks aerospace and defense contractors worldwide while misusing LinkedIn and WhatsApp.

[141] U.S. Department of Justice (2018, September 6). North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.

[142] Young, B., J. (2022, February 9). North Korea Knows How Important Its Cyberattacks Are.

The EU and U.S. can work together to deter conflict by conveying to North Korea the costs for any provocations through cyberattacks. Such a joint response from Western allies is far stronger than a unilateral approach and will help raise costs for North Korea. Additionally, the transatlantic partners and their government cybersecurity entities should be more direct in highlighting Chinese support of North Korean hackers when possible. Building stronger capabilities to counter and attribute attacks from North Korea is foundational to a transatlantic response.

Recommendations: Expand Cyber Norms and Diplomacy with the transatlantic partners

- **Embed a transatlantic focus in U.S. cyber diplomacy:** Appoint a senior official in the State Department's Bureau of Cyberspace and Digital Policy to focus on deepening the transatlantic cyber relationship. This appointment is critical to showcase that the U.S. is committed to pushing back on Russia's offensive cyber actions and to establishing norms through a closer diplomatic partnership with the EU. As opposed to tasking an existing senior official in the bureau, a new position also symbolizes the strategic prioritization of transatlantic cyber cooperation in a way that is otherwise not possible. This is of key importance to institutionalize the efforts and to signal to the Europeans that the U.S. takes transatlantic cyber diplomacy seriously. To support this perception among allies and adversaries alike, the appointment should coincide with the next *EU-U.S. Cyber Dialogue.*

- **Create an EU and U.S. cyber capabilities fund:** Through the *EU-U.S. Cyber Dialogue* and the TTC, create a new entity to deliver funding for cyber capacity-building projects in developing countries and emerging economies. This entity can also provide expert support and technical cybersecurity advice for developing robust capabilities. This could include funding the use of technical tools such as *Malware Information Sharing Platforms* (MISP), which allow for easier and standardized sharing of information between participating countries. One should also build on existing funding capacity-building programs, such as the *European Neighborhood Instrument* and the I*nstrument of Pre-Accession Finances Program*. Key development agencies to help build the cybersecurity and development nexus should be included. Along these lines, USAID's *Digital*

Development Program and the European Development Agency should be engaged for strategic advice and direction.

- **Increase transatlantic public diplomacy efforts:** *EU Cyber Direct* and the U.S. State *Department Bureau of Cyberspace* and *Digital Policy* should launch strategic awareness campaigns that build on the EU-U.S. alliance. The awareness campaigns should emphasize the importance of robust cybersecurity for the survival of Western democracy. The launch of a transatlantic advertising campaign highlighting the threat environment and individual-level action steps that citizens can take to secure their data should be coordinated. This campaign should focus on the short-term impact of Russia's ongoing cyberattacks in Ukraine and integrate the long-term strategic threats posed by China and other adversaries.

- **Strengthen international norm building efforts:** Leverage efforts like the OECD *Global Forum on Technology* and the *Paris Call* to advance international norms for responsible action in cyberspace and principles of non-proliferation of offensive cyber capabilities. For example, both the U.S. and EU should more actively support the *Paris Call* and encourage allies, European countries, and private sector companies to join the call. Through the *EU-U.S. Cyber Dialogue*, include a line of effort to begin discussions for establishing a set of norms for cyber policy and responses to gray zone tactics that accounts for the domain's evolving complexity and new threats from Russia and China.

Recommendations: Coordinate technical standards-based policy and regulations

- **Engage the U.S. in the EU Cybersecurity Certification Commission:** The most recent *EU-U.S. Cyber Dialogue* stressed the need for more collaboration on technical standards. Even with these public commitments, technical standards remain disparate and continue to cause friction. There is a unique window of opportunity with the ongoing creation of the EU Cybersecurity certification framework for ICT products. CISA, NIST, and the EU-wide Certification Framework Commission should establish a working group to integrate transatlantic coordination and provide recommendations for the EU Commission, prioritizing a security-by-design approach. Through this initiative, the U.S. and EU can work in tandem to identify areas for coordination in technical standardization, as opposed to a reactive approach that would take place after the Commission announces the updated framework.

- **ENISA transatlantic working group:** In tandem with the proactive coordination with the EU Commission, the ENISA Executive Director should establish an ENSIA ad hoc Working Group composed of experts from across the transatlantic cybersecurity community to review and identify technical regulations that cause the most friction in information sharing or capability expansion between the U.S. and EU. The final product of this working group should be a regulatory landscape overview for cyber policy experts and policymakers to leverage for promoting regulatory alignment. Additionally, the working group should build more points of connection between ENISA and U.S. cybersecurity entities. With ENISA's new permanent mandate, it is critical for transatlantic coordination to be institutionalized during the current phase of growth and mandate expansion.
- **Engage private sector feedback:** Work with the *U.S. Chamber of Commerce* and the *European American Chamber of Commerce* to advocate for the common interest of establishing the interoperability of respective digital systems and platforms and cybersecurity frameworks to ensure that transatlantic trade is not impeded. Invite both organizations to a roundtable discussion with cybersecurity experts for a listening session on private sector priorities for technical standards and for implementing security-by-design efforts.

Conclusion

Due to the transnational nature of cyberattacks, international cooperation is key to address the arising challenges to the information landscape, critical infrastructure, the economy, and overall security. In the context of the war in Ukraine and of China's increasingly advanced cyber capabilities, deeper transatlantic cooperation is important to curtail Russia's war ambitions and to defend economic, technological, political, and military infrastructure against adversarial attacks. The current moment of unmatched transatlantic unity in supporting Ukraine and strengthening cyber defenses presents a unique opportunity to overcome past political disagreements on related issues such as the regulation of big tech, data privacy, and cloud computing.

To capitalize on this momentum, the EU and the U.S. should embark on a path of greater social media regulation related to disinformation, institutionalization of big tech support in cyber defense, intelligence sharing, standardization of cyber governance guidelines, embrace of transatlantic public-private partnerships, and international funding for related endeavors. The transatlantic partners cannot afford to waste this moment in history; for the sake of the Ukrainian people and all those that believe in a democratically governed cyberspace. Amid the war in Ukraine, it is of urgent importance that cyber defenses are lastingly bolstered through continued transatlantic support. Stronger resiliency and cybersecurity measures can reduce human suffering, and allow for resources to be focused on Ukraine's kinetic defense.

At present, there is still time for deterrence as it relates to protecting transatlantic critical infrastructure. Alongside unprecedented transatlantic unity, this moment might pass. Considering the potentially increased role cyberwarfare will play in future conflicts, and given predictions that Chinese cyber capabilities will pose more far-reaching challenges than those of the Russians, the EU and the U.S. need to meaningfully increase their cyber cooperation now.

Bibliography

Adee, S. (2019, May 14). The global internet is disintegrating. What comes next? Retrieved March 2, 2023 from https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

Amazon (2022, June 9). Safeguarding Ukraine's data to preserve its present and build its future. Retrieved March 30, 2023 from https://www.aboutamazon.eu/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

Anagnostakis, D. (2021) The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. In Journal of Cyber Policy, 6:2, 243-261. Retrieved February 2, 2023 from https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1916975?cookieSet=1

Atkins, S. (2022, August 30). A web of partnerships: Ukraine, operational collaboration, and effective national defense in cyberspace. Washington, D.C.: Atlantic Council. Retrieved March 6, 2023 from https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/a-web-of-partnerships-ukraine-operational-collaboration-and-effective-national-defense-in-cyberspace/

Atlantic Council (2023). Undermining Ukraine: How the Kremlin Employs Information Operations to Erode Global Confidence in Ukraine. Washington, D.C.: Atlantic Council. Retrieved February 28, 2023 from https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Undermining-Ukraine-Final.pdf.

Bateman, J. (2022, December 16). Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences and Implications. Washington D.C.: Carnegie Endowment for International Peace. Retrieved March 2, 2023 from https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

BBC News (2022, March 5). War in Ukraine: Thousands march in Kherson against occupiers. Retrieved February 28, 2023 from https://www.bbc.com/news/world-europe-60632587.

BBC News (2022, February 6). North Korea: Missile programme funded through stolen crypto, UN report says. Retrieved March 10, 2023 from https://www.bbc.com/news/world-asia-60281129.

BBC News (2021, February 17). China overtakes US as EU's biggest trading partner. Retrieved March 3, 2023 from https://www.bbc.com/news/business-56093378.

Blair, D.C., Huntsman, J. M. (2013). The Report of the Commission on the Theft of American Intellectual Property. Washington, D.C.: National Bureau of Asian Research. Retrieved March 2, 2023 from https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf.

Canadian Centre for Cyber Security (2022, July 14). Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine. Retrieved October 27, 2022 from https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine

Carvin, S. (2022, September 22). Is Ukraine the Cyberwar That Wasn't? Waterloo: Centre for International Governance Innovation. Retrieved April 4, 2023 from https://www.cigionline.org/articles/is-ukraine-the-cyberwar-that-wasnt/

CERT-EU, ENISA (2023, February 15). JP-23-01 - Sustained activity by specific threat actors. Retrieved February 21, 2023 from https://cert.europa.eu/files/data/TLP-CLEAR-JointPublication-23-01.pdf

CERT-EU (2023). About us. Retrieved February 20, 2023 from https://cert.europa.eu/about-us

Cerulus, L. (2020, October 20). US calls out Russia for Macron campaign hack, even as France stays silent. Retrieved October 6, 2022 from https://www.politico.eu/article/us-russia-macron-campaign-hack-2017-election-france-attribution-gru/

Chang, E. (2022, July 5). Microsoft Shows Its Power Against Russia. Retrieved March 7, 2023 from https://www.thestreet.com/technology/microsoft-defending-ukraine-from-cyber-attacks

Chinese Ministry of Foreign Affairs & Cyberspace Administration of China (2017). International Strategy of Cooperation on Cyberspace. Retrieved March 1, 2023 from https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm.

Coble, S. (2022, February 24). Ukraine Attacked with Wiper Malware. Retrieved February 22, 2023 from https://www.infosecurity-magazine.com/news/ukraine-attacked-with-wiper-malware/.

Corera, G. (2022, April 7). Mystery of alleged Chinese hack on eve of Ukraine invasion. Retrieved February 21, 2023 from https://www.bbc.com/news/technology-60983346.

Corfield, G. (2023, January 7). Russian cyberattacks on Ukraine halved with help from Amazon and Microsoft. Retrieved March 7, 2023 from https://www.telegraph.co.uk/business/2023/01/07/russian cyberattacks-ukraine-halved-help-amazon-microsoft/

Council of Europe (2001). The Budapest Convention (ETS no. 185) and its Protocols. Strasbourg: Council of Europe. Retrieved February 20, 2023 from https://www.coe.int/en/web/cybercrime/the-budapest-convention

Council on Foreign Relations (2022). Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. Washington, D.C.: Council on Foreign Relations. Retrieved January 8, 2023 from https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

Council on Foreign Relations (n.d.). NotPetya. Washington, D.C.: Council on Foreign Relations. Retrieved February 2, 2023 from https://www.cfr.org/cyber-operations/notpetya.

CrowdStrike (2023). 2023 Global Threat Report. Retrieved March 4, 2023 from https://www.crowdstrike.com/global-threat-report/.

CSIS International Security Program (2019, July 8). By Other Means: Campaigning in the Gray Zone. Washington, D.C.: Center for Strategic and International Studies. Retrieved February 26, 2023 from https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone

CyberPeace Institute (2023). Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q4 October to December 2022. Retrieved March 1, 2023 from https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf

CyberPeace Institute (2022a). Case Study: Viasat. Retrieved March 1, 2023 from https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

CyberPeace Institute (2022b). Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q3 July to September 2022. Retrieved March 1, 2023 from https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q3%20Report.pdf

Delegation of the European Union to the PRC (2022, March 18). Disinformation About Russia's invasion of Ukraine – Debunking Seven Myths spread by Russia. Retrieved October 17, 2022 from https://www.eeas.europa.eu/delegations/china/disinformation-about-russias-invasion-ukraine-debunking-seven-myths-spread-russia_en?s=166

Dress, B. (2022, April 15). North Korean group stole more than $600M in Axie Infinity hack, FBI says. Retrieved March 10, 2023 from https://thehill.com/policy/cybersecurity/3269726-north-korean-group-stole-more-than-600m-in-axie-infinity-hack-fbi-says/.

ENISA, CERT-EU. (2023, February 15). Sustained Activity by specific threat actors. Retrieved April 28, 2023 from https://cert.europa.eu/static/files/TLP-CLEAR-JointPublication-23-01.pdf

ENISA (2023). Supporting Policy Developments to Achieve a High Common Level of Cybersecurity. Athens: European Union Agency for Cybersecurity. Retrieved February 23, 2023 from https://www.enisa.europa.eu/news/supporting-policy-developments-to-achieve-a-high-common-level-of-cybersecurity.

Erlich, A., Garner, C. (2023). Is pro-Kremlin Disinformation Effective? Evidence from Ukraine. In The International Journal of Press/Politics, 28 (1), 5-28. Retrieved February 28, 2023 from https://journals.sagepub.com/doi/pdf/10.1177/19401612211045221.

ESET (2022, June 1). ESET Research: Lazarus attacks aerospace and defense contractors worldwide while misusing LinkedIn and WhatsApp. Retrieved March 7, 2023 from https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-lazarus-attacks-aerospace-and-defense-contractors-worldwide-while-misusing-linkedin-a/

Euronews (2023, January 26). Russian hackers launch cyberattack on Germany in Leopard retaliation. Retrieved February 23, 2023 from https://www.euronews.com/2023/01/26/russian-hackers-launch-cyberattack-on-germany-in-leopard-retaliation

European Commission (2023, January 16). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Brussels: European Commission. Retrieved March 2, 2023 from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

European Commission (2022, December 19). Stakeholder Cybersecurity Certification Group. Brussels:

European Commission. Retrieved February 28, 2023 from https://digital-strategy.ec.europa.eu/en/policies/stakeholder-cybersecurity-certification-group#:~:text=The%20Stakeholder%20Cybersecurity%20Certification%20Group's,the%20European%20cybersecurity%20certification%20framework.

European Commission (2022, December 16). Cybersecurity: EU holds 8th dialogue with the United States. Brussels: European Commission. Retrieved February 26, 2023 from https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-holds-8th-dialogue-united-states.

European Commission (2022, June 7a). The Cybersecurity Strategy. Brussels: European Commission. Retrieved March 1, 2023 from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

European Commission (2022, June 7b). Joint Cyber Unit. Brussels: European Commission. Retrieved March 2, 2023 from https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

European Commission (2022, March 24). Joint Statement by President von der Leyen and President Biden. Brussels: European Commission. Retrieved February 27, 2023 from https://ec.europa.eu/commission/presscorner/detail/en/statement_22_2007.

European Commission (2019, March 12). EU-China strategic outlook: A joint contribution by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Council. Brussels: European Commission. Retrieved April 1, 2023 from https://commission.europa.eu/publications/eu-china-strategic-outlook-commission-and-hrvp-contribution-european-council-21-22-march-2019_en

European Commission (2017, September 13). Proposal for a Regulation of the European Parliament and of the Council on ENISA , the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). Brussels: European Commission. Retrieved February 22, 2023 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN.

European Cybersecurity Competence Centre and Network (n.d.). About us. Bucharest: European Cybersecurity Competence Centre and Network. Retrieved February 24, 2023 from https://cybersecurity-centre.europa.eu/about-us_en.

European Union External Action Service (2023, April 13). My view: China and EU-China relations. Brussels: European Union External Action Service. Retrieved March 3, 2023 from https://www.eeas.europa.eu/eeas/my-view-china-and-eu-china-relations_en.

European Union External Action Service (2022, January 24). The European Union Military Staff. Brussels:

European Union External Action Service. Retrieved February 20, 2023 from https://www.eeas.europa.eu/eeas/european-union-military-staff-eums_en

Europol (2022, March 1). European Cybercrime Centre - EC3. The Hague: Europol. Retrieved February 20, 2023 from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Faaborg-Andersen, S., Temes, L. (2022). The Geopolitics of Digital Standards. Cambridge: Belfer Center for Science and International Affairs. Retrieved March 2, 2023 from https://www.belfercenter.org/publication/geopolitics-digital-standards

Federal Bureau of Investigation (2019). Executive Summary - China: The Risk to Corporate America. Washington, D.C.: Federal Bureau of Investigation. Retrieved February 28, 2023 from https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf

Fivenson, A., Petrenko, G., Víchová, V., Poleščuk, A. (2023). Shielding Democracy: Civil Society Adaptations to Kremlin Disinformation about Ukraine. Washington, D.C.: National Endowment for Democracy. Retrieved March 7, 2023 from https://www.ned.org/wp-content/uploads/2023/02/NED_FORUM-Shielding-Democracy.pdf.

France24 (2023, March 13). Ukraine war fears give eastern Europe's populists new ammo. Retrieved April 26, 2023 from https://www.france24.com/en/live-news/20230313-ukraine-war-fears-give-eastern-europe-s-populists-new-ammo

Garamone, J. (2021, June 2). Official Talks DOD Policy Role in Chinese Pacing Threat, Integrated Deterrence. Arlington: U.S. Department of Defense. Retrieved February 12, 2023 from https://www.defense.gov/News/News-Stories/Article/Article/2641068/official-talks-dod-policy-role-in-chinese-pacing-threat-integrated-deterrence/

Geers, K. (2020). Case Study: Defending Democracy in Ukraine. In Alliance Power for Cybersecurity, 11-16. Washington, D.C.: Atlantic Council. Retrieved October 12, 2022 from https://www.jstor.org/stable/resrep26031.

Gibbons-Neff, T., Yermak, N. (2022, June 17). Russians Breached This City, Not With Troops, but Propaganda. Retrieved February 28, 2023 from https://www.nytimes.com/2022/06/17/world/europe/ukraine-russia-propaganda.html.

Google (2023). Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape. Retrieved March 1, 2023 from https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

Gordon, S., Rosenbach, E. (2021, December 14). America's Cyber-Reckoning: How to Fix a Failing Strategy. Retrieved February 14, 2023 from https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

Greig, J. (2023, February 17). Multiple Chinese APTs are attacking European targets, EU cyber agency warns. Retrieved April 28, 2023 from https://therecord.media/multiple-chinese-apts-are-attacking-european-targets-eu-cyber-agency-warns

Holder, J., Leatherby, L., Troianovski, A., Cai, W. (2023, February 23). The West Tried to Isolate Russia. It Didn't Work. Retrieved March 30, 2023 from https://www.nytimes.com/interactive/2023/02/23/world/russia-ukraine-geopolitics.html.

Huber, N. (2022, November 8). What Ukraine's cyber defence tactics can teach other nations. Retrieved March 7, 2023 from https://www.ft.com/content/9635c4a0-1f42-44f1-bc9a-503b192f809f

Hsu, P. (2018, January 23). Chinese Hacking Against Taiwan: A Blessing for the United States? Retrieved February 21, 2023 from https://thediplomat.com/2018/01/chinese-hacking-against-taiwan-a-blessing-for-the-united-states/.

Kharpal, A. (2022, March 9). China state-backed hackers compromised networks of at least 6 U.S. state governments, research finds. Retrieved April 28, 2023 from https://www.cnbc.com/2022/03/09/china-state-backed-hackers-compromised-6-us-state-governments-report.html

Kolmos, C. (2021, February 24). Bridging the Transatlantic Cyber Rift: Recommendations for Cyber Cooperation Between NATO and the EU. Washington, D.C.: Streit Council for a Union of Democracies. Retrieved April 20, 2023 from https://www.streitcouncil.org/post/bridging-the-transatlantic-cyber-rift-recommendations-for-improving-cyber-cooperation-between-nato

Langenkamp, A. (2022, May 8). From Russian rain to Chinese storm. Retrieved April 28, 2023 from https://thehill.com/opinion/national-security/3479964-from-russian-rain-to-chinese-storm/

Lyngaas, S. (2022, December 20). Kremlin-linked hackers tried to spy on oil firm in NATO country, researchers say. Retrieved March 2, 2023 from https://www.cnn.com/2022/12/20/politics/russia-ukraine-cyber-espionage-nato/index.html.

Lyngaas, S. (2022, November 5). Russian missile strikes overshadow cyberattacks as Ukraine reels from blackouts. Retrieved November 8, 2022 from https://www.cnn.com/2022/11/05/politics/russia-cyber-attacks-missiles-ukraine-blackouts/index.html

Maj Gen PK Mallick, VSM (2022). Decoding Russia's "Missing" Cyberwar Amid War in Ukraine. Retrieved April 3, 2023 from https://www.vifindia.org/sites/default/files/Decoding-Russia-s-Missing-Cyberwar-Amid-War-in-Ukraine.pdf

McLaughlin, J. (2023, March 3). Russia bombards Ukraine with cyberattacks, but the impact appears limited. Retrieved March 3, 2023 from https://www.npr.org/2023/02/23/1159039051/russia-bombards-ukraine-with-cyberattacks-but-the-impact-appears-limited

McMillan, R., Volz, D. (2023, March 16). Wave of Stealthy China Cyberattacks Hits U.S., Private Networks, Google says. Retrieved April 24, 2023 from https://www.wsj.com/articles/wave-of-stealthy-china-cyberattacks-hits-u-s-private-networks-google-says-2f98eaed

Menn, J., Timberg, C. (2022, February 28). The dire predictions about a Russian cyber onslaught haven't come true in Ukraine. At least not yet. Retrieved April 2, 2023 from https://www.washingtonpost.com/technology/2022/02/28/internet-war-cyber-russia-ukraine/

Metz, C. Vinograd, C., Cooper, H. (2022, October 14). Elon Musk Foments More Geopolitical Controversy With Ukraine Internet Dispute. Retrieved April 28, 2023 form https://www.nytimes.com/2022/10/14/technology/elon-musk-ukraine-internet.html

Microsoft (2022, November 4). Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression. Retrieved February 27, 2023 from https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/#:~:text=Nation%2Dstate%20cyberattacks%20become%20more%20brazen%20as%20authoritarian%20leaders%20ramp%20up%20aggression,-Nov%204%2C%202022&text=On%20February%2023%2C%202022%2C%20the,and%20digital%20attacks%20against%20Ukraine.

Microsoft (2022, June 22). Defending Ukraine: Early Lessons from the Cyber War. Retrieved February 22, 2023 from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

Microsoft (2022, April 27). Special Report: Ukraine - An overview of Russia's cyberattack activity in Ukraine. Retrieved October 23, 2022 from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Miller, M. (2023, January 15). Ukraine calls for “Cyber United Nations” amid Russian attacks. Retrieved February 28, 2023 from https://www.politico.com/news/2023/01/15/ukraine-cyber-united-nations-russia-00077955

Miller, M. (2023, January 11). Russia’s cyberattacks aim to “terrorize” Ukrainians. Retrieved February 1, 2022 from https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561.

Murphy, M. (2022, December 21). Espionage, Not Blackouts, Is Theme of Russian Hacking in Ukraine. Retrieved March 2, 2023 from https://www.bloomberg.com/news/newsletters/2022-12-21/espionage-not-blackouts-is-theme-of-russian-hacking-in-ukraine.

Nye, J. S., Jr. (2022, June 15). Eight Lessons from the Ukraine War. New York: Project Syndicate. Retrieved October 18, 2022 from https://www.project-syndicate.org/commentary/russia-war-in-ukraine-eight-lessons-by-joseph-s-nye-2022-06?barrier=accesspaylog.

OECD (2022, November 3). Disinformation and Russia’s war of aggression against Ukraine: Threats and governance responses. Paris: Organization for Economic Cooperation and Development. Retrieved February 28, 2023 from https://www.oecd-ilibrary.org/docserver/37186bde-en pdf?expires=1677648273&id=id&accname=guest&checksum=F804491FB86FF97520EE6D135795C606.

Olterman, P. (2023, February 24). Leaders of German left condemn “peace rally” over far-right involvement. Retrieved February 28, 2023 from https://www.theguardian.com/world/2023/feb/24/leaders-of-german-left-condemn-peace-rally-over-far-right-involvement

Przetacznik, J., Tarpova, S. (2022). Briefing - Russia‘s war on Ukraine: Timeline of cyber-attacks. Brussels: European Parliamentary Research Service. Retrieved October 18, 2022 from https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Reuters (2022, December 26). Zelenskiy: power shortages persist, nearly 9 million Ukrainians without electricity. Retrieved March 2, 2023 from https://www.reuters.com/business/energy/zelenskiy-power-shortages-persist-nearly-9-million-ukrainians-without-2022-12-26/.

Reuters (2022, November 3). Microsoft extends free tech support through 2023. Retrieved March 7, 2023 from https://www.reuters.com/technology/microsoft-extends-free-tech-support-ukraine-through-2023-2022-11-03/

Reuters (2018, February 15). White House blames Russia for ‘reckless’ NotPetya cyber attack. Retrieved February 27, 2023 from https://www.reuters.com/article/us-britain-russia-cyber-usa/white-house-blames-russia-for-reckless-notpetya-cyber-attack-idUSKCN1FZ2UJ.

Roulette, J. (2023, February 9). SpaceX curbed Ukraine’s use of Starlink internet for drones - company president. Retrieved April 28, 2023 from https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/

Russia Matters (2022, May 4). Why Hasn’t Russia Unleashed “Cybergeddon” in Its War on Ukraine. Cambridge: Belfer Center for Science and International Affairs. Retrieved March 2, 2023 from https://www.russiamatters.org/analysis/why-hasnt-russia-unleashed-cybergeddon-its-war-ukraine

Sabbagh, D. (2023, January 19). Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency. Retrieved January 20, 2023 from https://www.theguardian.com/world/2023/jan/19/cyber-attacks-have-tripled-in-past-year-says-ukraine-cybersecurity-agency.

Santora, M. (2022, August 16). The operators of Ukraine's nuclear plants says it faced an ambitious cyberattack. Retrieved February 20, 2023 from https://www.nytimes.com/2022/08/16/world/europe/the-operator-of-ukraines-nuclear-plants-says-it-faced-an-ambitious-cyberattack.html

Scott, M. (2021, February 4). How Trump won over Europe on 5G. Retrieved February 1, 2023 from https://www.politico.com/news/2021/02/04/trump-europe-5g-466016

Seward, S. J. (2018). Cyberwarfare in the Tactical Battlespace: An Intelligence Officer'sPerspective. Fort Benning: US Army Fort Benning and the Maneuver Center of Excellence. Retrieved October 10, 2022 from https://www.benning.army.mil/Infantry/Magazine/issues/2018/Apr-Jun/PDF/7)Seward-Cyber_txt.pdf.

Sky News (2022, July 19). Russian cyber spies targeting NATO countries in new hacking campaign. Retrieved March 2, 2023 from https://news.sky.com/story/russian-cyber-spies-targeting-nato-countries-in-new-hacking-campaign-12654964.

Starks, T. (2023, February 16). What we've learned from a year of Russian cyberattacks in Ukraine. Retrieved March 2, 2023 from https://www.washingtonpost.com/politics/2023/02/16/what-we-learned-year-russian-cyberattacks-ukraine/.

Symantec (2022, February 28). Daxin: Stealthy Backdoor Designed for Attacks Against Hardened Networks. Retrieved March 2, 2023 from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage.

The White House (2023, March 1). National Cybersecurity Strategy. Washington, D.C.: The White House. Retrieved March 3, 2023 from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The White House (2022, October 12). National Security Strategy. Washington, D.C.: The White House. Retrieved March 1, 2023 from https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf

UN General Assembly (2022, March 2). Resolution adopted by the General Assembly on 2 March 2022 - Aggression against Ukraine. New York: United Nations. Retrieved February 21, 2023 from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/293/36/PDF/N2229336.pdf?OpenElement.

UN News (2023, February 23). UN General Assembly calls for immediate end to war in Ukraine. New York: United Nations. Retrieved February 24, 2023 from https://news.un.org/en/story/2023/02/1133847

U.S.-China Economic and Security Review Commission (2022). 2022 Annual Report to Congress. Washington, D.C.: U.S-China Economic and Security Review Commission. Retrieved March 6, 2023 from https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf.

U.S.-China Economic and Security Review Commission (2022, February 17). China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States. Washington, D.C.: U.S-China Economic and Security Review Commission. Retrieved March 6, 2023 from https://www.uscc.gov/hearings/chinas-cyber-capabilities-warfare-espionage-and-implications-united-statesU.S. Department of Energy (2022, August 17). DOE Announces $45 Million for Next-Generation Cyber Tools to Protect the Power Grid. Washington, D.C.: U.S. Department of Energy. Retrieved March 7, 2023 from https://www.energy.gov/articles/doe-announces-45-million-next-generation-cyber-tools-protect-power-grid

U.S. Department of Justice (2018, September 6). North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions. Washington, D.C.: U.S. Department of Justice. Retrieved March 1, 2023 from https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

U.S. Department of Justice (2020, September 16). Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally. Washington, D.C.: U.S. Department of Justice. Retrieved April 23, 2023 from https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

U.S. Department of State (2022, December 21). The 2022 U.S.-EU Cyber Dialogue Media Note. Washington, D.C.: U.S. Department of State. Retrieved March 2, 2023 from https://www.state.gov/the-2022-u-s-eu-cyber-dialogue/.

U.S. Department of State (2022, May 10). U.S. Support for Connectivity and Cybersecurity in Ukraine. Washington, D.C.: U.S. Department of State. Retrieved February 2, 2023 from https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/#:~:text=Prior%20to%20February%202022%2C%20the,capacity%20development%20assistance%20since%202017.

U.S. Office of the Director of National Intelligence (2021, April 9). Annual Threat Assessment of the US Intelligence Community. Washington, D.C.: Office of the Director of National Intelligence. Retrieved March 3, 2023 from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

U.S.: Senate Select Committee on Intelligence (2018, May 8). Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security. Washington, D.C.: U.S. Senate. Retrieved February 1, 2023 from https://www.intelligence.senate.gov/press/senate-intel-committee-releases-unclassified-1st-installment-russia-report-updated

van Sant, S. (2023, January 9). Kyiv argues Russian cyberattacks could be war crimes. Retrieved March 10, 2023 from https://www.politico.eu/article/victor-zhora-ukraine-russia-cyberattack-infrastructure-war-crime/

Verkhovna Rada of Ukraine (2021, March 23). About the creation of the Center for countering disinformation. Kyiv: Verkhovna Rada of Ukraine. Retrieved April 24, 2023 from https://zakon.rada.gov.ua/laws/show/n0015525-21#Text

Waterman, S. (2023, February 21). Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts. Retrieved March 9, 2023 from https://www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970.

Westby, J. (2020, December 20). Russia Has Carried Out 20-Years Of Cyber Attacks That Call for International Response. Retrieved October 4, 2022 from https://www.forbes.com/sites/jodywestby/2020/12/20/russia-has-carried-out-20-years-of-cyber-attacks-that-call-for-international-response/?sh=e2bde956605a

Wintour, P. (2023, February 28). China spends billions on pro-Russia disinformation, US special envoy says. Retrieved March 1, 2023 from https://www.theguardian.com/world/2023/feb/28/china-spends-billions-on-pro-russia-disinformation-us-special-envoy-says.

Xinhuanet (2019, April 22). Co-construction of the "Belt and Road Initiative": Progress, Contributions and Prospects. Retrieved March 7, 2023 from http://www.xinhuanet.com/world/2019-04/22/c_1124400071.htm.

Xinhuanet (2015, December 16). Speech by Xi Jinping at the Opening Ceremony of the Second World Internet Conference (full text). Retrieved February 27, 2023 from http://www.xinhuanet.com/politics/2015-12/16/c_1117481089.htm

Young, B., J. (2022, February 9). North Korea Knows How Important Its Cyberattacks Are. Retrieved April 29, 2023 from https://foreignpolicy.com/2022/02/09/north-korea-knows-how-important-its-cyberattacks-are/#:~:text=In%20internal%20regime%20discourse%2C%20Pyongyang,guarantees%20our%20military's%20capability%20to

Zabierek, L. (2022). The New Frontier of Democratic Self-Defense. Belgrade: Center for International Relations and Sustainable Development. In Horizons, Winter 2022 (20). Retrieved March 30, 2023 from https://www.cirsd.org/en/horizons/horizons-winter-issue-20/the-new-frontier-of--democratic-self-defense

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
www.belfercenter.org

Printed in the United States of America