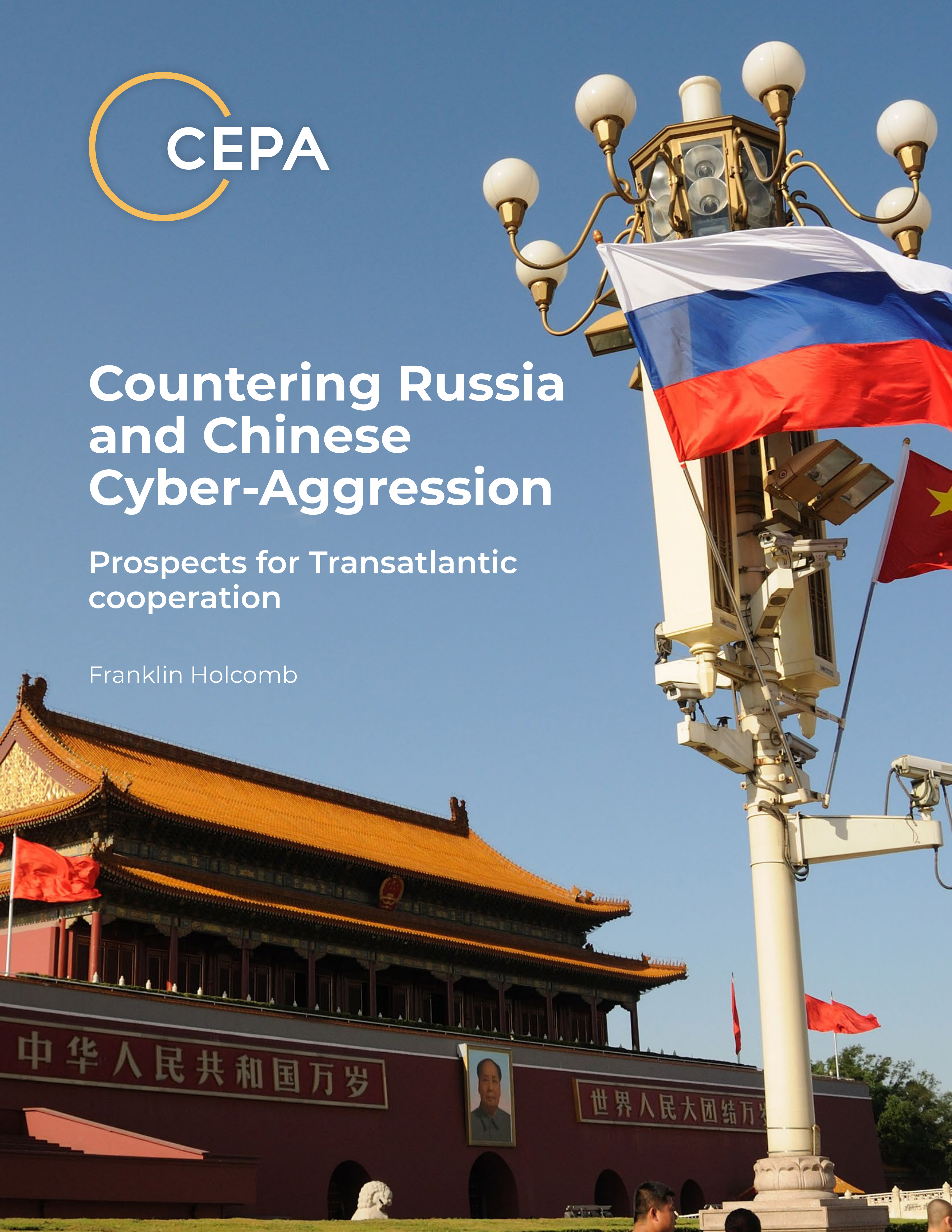
CEPA

Countering Russia and Chinese Cyber-Aggression

Prospects for Transatlantic cooperation

Franklin Holcomb



CONTENTS

ABOUT CEPA

The Center for European Policy Analysis (CEPA) works to reinvent Atlanticism for a more secure future. Headquartered in Washington, D.C., and led by seasoned transatlanticists and emerging leaders from both sides of the Atlantic, CEPA brings an innovative approach to the foreign policy arena. Our cutting-edge analysis and timely debates galvanize communities of influence while investing in the next generation of leaders to understand and address present and future challenges to transatlantic values and principles. CEPA is a nonpartisan, nonprofit, public policy institution.

All opinions are those of the author(s) and do not necessarily represent the position or views of the institutions they represent or the Center for European Policy Analysis.

Cover: Chinese and Russian national flags flutter on a lamppost on the Tian'anmen Square in Beijing, China, 24 June 2016. China is working for the establishment of an investment fund worth 100 billion yuan (15.3 billion U.S. dollars) to finance regional cooperation projects between China and Russia, Chinese Vice Premier Wang Yang said on Thursday (7 September 2017). China is ready to increase the scale of the investment fund and suggest the Silk Road Fund finance China-Russia joint programs, Wang said in a speech at a commercial conversation on the sidelines of the Third Eastern Economic Forum in Vladivostok, a major Pacific port city in Russia. He said the Chinese government encourages enterprises to invest in Russia's Far East and expand cooperation in manufacturing, resources exploitation, infrastructure, agriculture and tourism. Credit: REUTERS
.

ABOUT THE AUTHORS

Franklin Holcomb is a Title VIII Fellow in the Transatlantic Leadership program at CEPA with a focus on Russian and Eastern European security and political analysis.

Before joining CEPA, Franklin worked as an analyst at the Institute for the Study of War where he published multiple reports on Eastern European security, particularly focused on the Russian invasion of Ukraine. He also worked as an academic assistant at the Baltic Defense College in Tartu, Estonia as part of his master's degree studies.

Franklin graduated from Texas A&M University with a double major in Russian Language and International Studies: Politics and Diplomacy. He is finishing his master's degree in Democracy and Governance at the University of Tartu where he studied governance policy, including Estonia's e-Governance systems. His dissertation is focused on the analysis of the militias of Estonia, Latvia, and Lithuania. He has a deep interest in cybersecurity, particularly as it relates to political and military activity in Europe. Franklin has studied and lived in Russia and speaks advanced Russian as well as some Ukrainian.

Executive Summary

The United States and its European partners face serious and determined cyber opponents and must expand cyber defense cooperation with an emphasis on learning from each other's strengths.

- Russia has shown itself to be a reckless cyber actor, with its NotPetya cyberattacks against Ukraine in 2017 that devastated private and public systems worldwide.
- Cyber vulnerabilities to European countries are also vulnerabilities to the United States.
- Hostile cyber actors such as Russia and China have not been deterred by Western policy responses and the West must focus on becoming more resilient to cyberattacks.
- State-sponsored cyber operations, both hacking and disinformation, are increasingly mutually reinforcing.
- Eastern European states have taken innovative policy steps to harden their defenses against constant Russian cyber aggression.
- The U.S. government and U.S. civil society should expand their outreach to eastern European governments and societies to help support and learn from our partners and thereby improve our cyber defenses.

Introduction

The United States and its allies face increasingly capable and aggressive cyber opponents and must work together and learn from one another to counter them. Hostile countries regularly mount major cyber operations against American and European states aiming to disrupt their economies, conduct espionage, undermine military readiness and manipulate public opinion through the spread of disinformation. At the same time, Western societies are becoming ever more politically and economically interconnected through digitalization. The internet of things (IoT) is dramatically increasing the connectivity of the average citizen, with the number of IoT devices worldwide expected to hit 50 bn by 2022.[1] States too are becoming increasingly digitalized as they increasingly rely on e-services and data storage. As more people and services go online, hostile actors have exponentially more entry points for attacks, information to steal or distort, and systems to breach and paralyze.

Cyber threats to society cannot be contained to ensure they do not threaten the government, nor can a state isolate itself from threats to its allies and partners. A hostile breach of a café outside a parliament in Europe that exploits a vulnerability in an IoT device that the cashier did not update could be used in seconds to infect key systems, steal vital data from the target country and enable more dangerous attacks on American targets. Meanwhile, an attack on a café on Capitol Hill aimed at gaining access to a congressional staffer's phone poses the same risks to European states. As the internet erodes geographic restrictions on communication and trade and helps bring the Euro-Atlantic community closer together it also increases American and European vulnerabilities to interlinked cyberattacks, particularly coordinated operations from hostile governments. Because we are only as strong as our weakest link, as the maxim goes, cybersecurity cannot be thought of in purely national terms. If a disinformation campaign succeeds in undermining political stability in Europe, it is only a matter of time until a similar one is loosed on the United States. Increasing active cooperation between America and European countries, particularly in joint research, cyber-exercises and training, as well as efforts to develop common understanding of hostile cyber actors' intentions, are already crucial to securing our shared political, economic and military interests from hostile cyber activity and will only become more so in coming years.

WANTED BY THE FBI
GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS
Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft
Sergey Vladimirovich Detistov
Pavel Valeryevich Frolov

A poster showing six wanted Russian military intelligence officers is displayed as U.S. Attorney for the Western District of Pennsylvania Scott Brady, accompanied by Assistant Attorney General for the National Security Division John Demers, speaks at a news conference at the Department of Justice, in Washington, U.S., October 19, 2020. Credit: Andrew Harnik/Pool via REUTERS.

Background

Governments have used cyber tools to many ends, including conducting information operations to influence elections or political decisions, snooping to extract information, disrupting economies and supporting ongoing combat operations. The lines notionally dividing these operations were always weak and have eroded to the point that they are often differences without distinction.

Hostile actors now conduct multifaceted operations that do not fit easily within existing models of thinking about security. These attacks' long-term objectives, such as undermining American influence or European unity, often overlap and reinforce one another. Cyber operations targeting politicians in the United States can be used to gain access to governmental systems or to extract useful intelligence, but they can just as easily be used to extract information and release it as part of a wider disinformation operation targeting the U.S. and/or European publics. Russian cyber actors have conducted cyber "information operations commensurate with broader strategic military doctrine" by breaching a target organization and stealing "internet data that is then leaked to further political narratives aligned with Russian interests," the cybersecurity firm FireEye concluded in 2017.[2]

Cyber and information operations are increasingly linked and mutually reinforcing, complicating effective and coordinated response by traditional government agencies. "Cybersecurity isn't purely IT. Active operations are targeting people's minds in cyberspace,"[3] Joanna Świątkowska, the former program director of the European Cybersecurity Forum, observed. When considering how to help their countries withstand cyberattacks, policymakers should realize that cyber threats are a wide range of potential threats and operations against an entire society, with distinct yet often overlapping objectives.

Central and eastern European countries have been primary targets in modern cyber warfare since at least 2007, when a massive series of attacks, including distributed-denial-of-service attacks as well as more complex attempts to hack into specific systems, savaged Estonia in conjunction with widespread riots and vandalism conducted by ethnic Russians in the country.[4] Since then, hostile cyber operations originating from hostile states such as Russia and China with a wide range of political, economic and military objectives have repeatedly hit every country on the Continent. Most prominent among these attacks was the 2017 Russian NotPetya attack on Ukraine, which inflicted massive economic damage worldwide. Due to its Russian creators' negligence or malice, the attack spilled out of Ukraine, nearly crippling the international shipping giant Maersk and causing an estimated $10 bn in economic damages.[5] The United States indicted six members of Russia's military intelligence for conducting the attacks on Ukraine, among other dangerous cyber activity, though naming and shaming the individual hackers will hardly deter Russia from pursuing similar operations.[6]

Cyberattacks against countries in central and eastern Europe continue, and the region has become a laboratory for hostile cyber actors seeking to test new tools and methods of manipulation. Russia's attacks on Estonia in 2007, its attacks on the Ukrainian power grid with BlackEnergy in 2015 and NotPetya in 2017, and its ongoing cyber operations demonstrate the Kremlin's view of eastern Europe as a primary target for cyber operations.[7] "When they want to try something new, they try it on us and then think about if that kind of model can be used elsewhere, maybe someday in the U.S.," said Rolands Heniņš, Latvia's defense counselor in Washington.[8] Europe and America share cyber adversaries, prominently including Russia and China, who aim to exploit technical weaknesses and social strife.

Section 1: The Cyber Bear and Dragon

The cyber threat landscape is vast and increasingly active, and it endangers governments and citizens on both sides of the Atlantic. Among the wide array of hostile entities, Russia and China pose unique threats to the Euro-American alliance. Central and eastern European governments and societies are under increasing pressure from these hostile states, who disrupt, compromise and exploit European cyberspace to undermine Western societies and further their own political ends. Russia and China aim to expand their global influence at the expense of the United States and its partners.[9] Although they use different tools to pursue different goals, they both work to weaken the transatlantic alliance and democratic norms. Of the two, Russia is the more reckless and poses the greater danger to the democratic community today. China is somewhat less obviously aggressive in cyberspace, yet it could surpass Russia as the democratic world's primary cyber threat at some point in the 21st century.

The Cyber Bear

With its history of aggression toward American allies in Europe, Russia is the Euro-Atlantic community's most dangerous cyber opponent. The Kremlin is a committed, hostile, reckless and inventive actor that will require coordinated, consistent and committed transatlantic cooperation to manage.

The Russian government views the American-European partnership as a threat to its regional and global interests, and it has committed to an adversarial relationship with the United States and its European allies. Putin's primary aims include the "preservation of his regime, the end of American global hegemony and the restoration of Russia as a mighty and feared force on the international stage."[10] While the Russian government is not always a unitary actor, Putin's core objectives unite the often feuding and disparate components of its foreign policy, military, and intelligence apparatus and are consistently pursued by all branches of state.[11] Putin's Russia sees the American-European partnership as a key roadblock to pursuing its revanchist dream of turning Russia into a political and military power that dominates or controls its neighbors in Europe. The Putin regime views democratic projects across former-Soviet territory as a unique and primary threat to its domestic legitimacy and regional influence. The regime wages complex military, economic, political and intelligence campaigns against these projects, despite international sanction and condemnation.

The Kremlin has shown little compunction about using any means at its disposal, including its cyber toolkit, to antagonize the United States, undermine democratic countries and attempt to assert control in Europe. The Russian government extensively uses disinformation and hacking to achieve political, economic or military ends. Military operations against Ukraine and Georgia aimed at punishing these countries for their lack of fealty to Moscow have been accompanied by devastating hacking operations against targets such as electrical grids, government websites, corporations, and even frontline artillery units.[12] European countries, including France in 2017, which was targeted by a Russian hack-and-dump operation against then-candidate Emmanuel Macron, have been repeatedly targeted by Russian hackers working with disinformation campaigns to influence the results of local and national elections.[13] Countries in Europe with national agendas that Russia views as counter to its global interests, such as Poland, Romania, Norway and others, have been targeted by Russian cyberattacks and political pressure simultaneously.[14]

Russian cyber actors are sophisticated and committed. According to Nicu Popescu, Moldova's minister of foreign affairs and European integration, and Stanislav Secrieru, a senior analyst at the European Union Institute for Security Studies, Russia has a long history of activity in cyberspace and is "undoubtedly one of the world's great cyber powers" with "extremely sophisticated capabilities" that are "integrated into its foreign and security policy much more extensively than other international players."

That virtuosity is thanks in part to a "general laissez-faire approach to cybersecurity" by the international community.[15] During this period of relative inattention to Russia's cyber campaigns, the Kremlin has used its cyber tools in reckless and dangerous ways particularly against Ukraine. The Kremlin conducted cyberattacks against civilian infrastructure in Ukraine in 2015, crossing a de facto red line. The Kremlin's attacks on Ukraine in 2017 not only caused immense damage to Ukraine but resulted in massive spillover well beyond the scope of its initial attack, causing worldwide economic chaos.

The Cyber Dragon

China, another global cyber superpower, has worked to shore up its image in central and eastern Europe as part of a larger effort to thwart any global moves to check its activity worldwide. While its aim has been less obviously aggressive and confrontational than Russia's, China nevertheless poses long-term threats to the unity of the European bloc and the transatlantic alliance.

With primarily economic and political interests in Europe, China seeks "influence over political parties and politicians" and to make the Continent more dependent on Chinese technology, according to Veronika Víchová, the head of KremlinWatch at the European Values Center for Security Policy.[16] "Chinese economic influence might not be

Abraham Liu, Huawei Chief Representative to the EU Institutions and Vice-President European Region speaks at a news conference at the Huawei European Cybersecurity Center in Brussels, Belgium, May 21, 2019. Credit: REUTERS/Francois Lenoir.

an immediate risk to European politics, but the attraction of Chinese investment could pose a medium-to-long term threat to the EU and transatlantic community if it leads to individual members trying to break European consensus on Chinese foreign policies," Víchová said.[17]

China's footprint in European cyberspace has so far been smaller than Russia's, though recent developments, including the coronavirus crisis, suggest it could be set to expand. China has used cyberspace to spy in Europe, prominently targeting EU diplomatic cables.[18] The regime in Beijing has developed sophisticated cyber hacking operations looking for ways to blackmail or sway key politicians in Europe to look more kindly on Chinese geopolitical interests, said Janusz Bugajski, a senior fellow at the Center for European Policy Analysis.[19] In addition, since the beginning of the coronavirus crisis, China has churned out more Covid-related disinformation, and senior EU leaders have suggested a link between China and attempted hacks of European hospitals.[20] All of which makes China's efforts to entrench state-linked firm Huawei into European telecommunications infrastructure all the more concerning for Europe's long-term security.[21]

Section 2: European Innovation and Strengths in Cyber Defense

After more than a decade in the crosshairs of hackers and online snoops, central and eastern European governments, businesses and civil society groups have developed a wealth of expertise and institutional knowledge on cyber defense. Cyber defense capacity and innovation has not developed uniformly across Central and

Eastern Europe, and many states have only recently started to make great strides in improving their cyber capacity as part of a general wake-up. Edvinas Kerza, a former deputy defense minister of Lithuania, said his government realized that "you can lose a war or a battle without the firing of a single bullet" as cyber adversaries use cheap-to-produce viruses to do "as much damage as missiles" against unprepared targets.[22] In response, experts and others in the region have pioneered policy systems and principles that can serve as models for hardening cyber defenses worldwide and as frameworks for enhancing U.S.-European cyber cooperation against shared threats.

Of course, strengthening cybersecurity is a complex undertaking that requires the participation of not only the government but also businesses, civil society organizations and ordinary citizens. If any one of these layers is vulnerable to cyber exploitation through hacking or disinformation, it invariably endangers the others. It is important, then, to remove institutional barriers that artificially silo state entities from one another and from the rest of society.

Some central and eastern European countries are working at all levels, from consulting internationally to fostering domestic civilian responses, to ward off or respond to cyber threats. Without the financial and scientific resources of the United States, countries in the region have had to come up with creative approaches to this problem. Their answers are not necessarily replicable elsewhere but they nevertheless provide a framework for thinking about and improving cybersecurity on multiple levels of society.

Societal Level

A government's cybersecurity is inherently tied to the level of cyber resilience in the society it governs. Thus, ensuring societal buy-in to cybersecurity practices, helping people spot and resist disinformation campaigns, and using civilian talent to supplement state capacity are crucial. Organizations and governments across central and eastern Europe have launched important initiatives and built policy systems to achieve these goals.

Cyber Auxiliaries

Estonia, Latvia and Lithuania's state-run auxiliary cyber units grew out of conventional civilian defense reserves, ready to be called up in times of crisis. As the nature of threats has evolved, these units have added cyber expertise to their arsenal and have worked to raise awareness of cybersecurity and threats among their fellow citizens.

The three main units, the Estonian Defense League (Kaitseliit), Latvian National Guard (Zemessardze) and Lithuanian Riflemen's Union (Lietuvos Šaulių Sąjunga), are generally led or overseen by state authorities. In a conflict or crisis, the Baltic states can mobilize tens of thousands of people into ready-built units with deep knowledge of local terrain and communities. They are trained in a wide range of activities, from support operations and frontline combat to organizing guerrilla activities and resistance movements—and now, with the increasing digitalization of society, to protecting Baltic societies in cyberspace from cyberattacks and disinformation.[23]

The Baltic auxiliaries play a key role in regional cyber defense as professional hubs, training grounds, and most importantly, institutions where patriotic civilians who might not be willing to commit to a military lifestyle can support national armed forces' cyber defense capabilities. Olevs Nikers, president of the Baltic Security Foundation, said the Latvian National Guard's cyber unit "serves as a great hub for countering, detecting and raising the alarm about issues faced by the armed forces" while helping to "build expertise and train new people."[24] By bringing civilian experts into cyber defense, the Baltic states have not only enhanced state cyber capacity but also fostered a whole-of-society approach to the issue.

Counter Disinformation Movements

The threats posed by disinformation to Western societies and political structures have become increasingly clear in recent years. Hostile disinformation campaigns have run the gamut from attacks on NATO, such as recent operations by Russia-linked hackers to push disinformation about NATO in Poland and Lithuania, to now-infamous operations against the U.S. electorate.[25] Countries across central and eastern Europe, however, have been on the geographic and metaphorical front line in the fight against disinformation for over a decade. Many civil society groups and eastern European governments have developed hard-earned experience while serving as a testing ground for hostile disinformation campaigns. Among the lessons learned: State-led responses, while often helpful, may be insufficient in countering disinformation, so civil initiatives have stepped in to spot, uncloak and counter hostile disinformation campaigns.

Organizations such as Propastop, the Czech Elves, the Baltic Elves and others have played key roles in educating people about disinformation. These groups, started by patriotic and civic-minded experts and journalists across eastern Europe, use advanced technologies and expert knowledge to stop the spread of dangerous hostile narratives. For example, Kerza said the Baltic Elves use a specialized AI to monitor social networks and news portals that can detect possible disinformation within two minutes of it being posted. Their experts then search these results for specific trends and publicly identify the attempted disinformation campaigns.[26] While technical wizardry no doubt makes this work easier and more effective, the heart of any effort to counter disinformation is a corps of knowledgeable and committed experts.

National Level

Governments across eastern Europe have taken important steps to bolster their cyber defenses by securing key state data, streamlining and fine-tuning their responses to hostile cyber action, and linking up the region's officials and experts to confront joint challenges.

Estonia's Data Embassies

While no system or data is ever fully secure, ensuring government continuity is not disrupted by data loss in the event of a major real-world or cyber crisis is crucial. Committed and competent attackers can eventually compromise nearly any system. As societal and government workflows become ever more digitized, more key data becomes vulnerable to hostile cyberattacks, while physical attacks on key servers also remain a threat to government functions.

In response, the government of Estonia has pioneered an innovative approach to security by establishing a "data embassy" in Luxembourg. Data embassies, which have the same rights as traditional embassies, are "servers outside the country that are legally under Estonian jurisdiction" in which digital copies of key databases are stored and secured against hostile attack.[27] The former director of the International Centre for Defence and Security (ICDS) in Tallinn, Sven Sakkov, said the embassy "Is an additional layer of resilience ... it's like having your phone doing automatic backups regularly" and noted that "it gives us the ability to reboot services even if something bad happens."[28] Estonia's data embassy complicates any cyber operation aimed at crippling the government's access to its data, and helps ensure that the data is not destroyed or seized by hostile forces in a conflict or temporary foreign occupation.

A woman looks at the screens during the Locked Shields, cyber defence exercise organized by NATO Cooperative Cyber Defence Centre of Exellence (CCDCOE) in Tallinn, Estonia April 10, 2019. Credit: REUTERS/Ints Kalnins.

Consolidated State Cyber Authority

Rapid and decisive action and a clear chain of responsibility are important to ensuring a state can respond to a hostile cyberattack quickly and effectively. Excessive siloing or duplication of cyber efforts in different agencies can hamstring a state's capacity to halt a major attack and mitigate damage.

Lithuania has benefited from efforts to centralize its cyber command. In 2015, it ranked 50th on the International Telecommunication Union's Global Cybersecurity Index, but thorough efforts to rethink its cybersecurity command structures vaulted it to fourth place in 2018.[29] Edvinas Kerza, the former deputy defense minister, said Lithuania reformed its cybersecurity policies after seeing serious Russian cyberattacks on Georgia and Ukraine. Lithuania "stopped viewing cybersecurity in separate pieces," he said, with different responsibilities "going to the Interior Ministry, the Ministry of Transport, the Foreign Ministry, and so on." Though the government consolidated cyber defense in the Defense Ministry's National Cyber Security Center, not all participants are military officers, and civilians occupy high-ranking posts in cyber decision-making.[30] With responsibility for Lithuania's cyber defense concentrated in one place, Kerza said, "We joined forces in one center and started doing a practical job, not pointing fingers and trying to delegate responsibility." Streamlining its cyber forces and command structures has made the country much more resilient to cyberattacks or mischief, but Kerza stressed that its cyber forces are distributed throughout the country with multiple layers of redundancy, including Lithuania's auxiliaries, EU institutions and NATO, to thwart a possible cyber-decapitation strike.[31]

International Cooperation

Cyberattacks pose serious risks not only to their primary target, but also to countries with economic, social, military or political ties to the target, necessitating a multinational response to cybersecurity. Countries across central and eastern Europe, working multilaterally or through NATO or the EU, have built the expert-to-expert ties necessary to boost cyber capacity and ensure that none of them is ever alone against a cyberattack.

Training centers where experts from across NATO and NATO-partner states can meet to share experience and conduct research and training are critical. Four centers in Estonia, Latvia and Lithuania produce nuanced analysis of hostile cyber campaigns and bolster regional capacity to counter hostile hacking and information operations.

Information Warfare:

- The NATO StratCom Center of Excellence in Riga was established in 2014 by Estonia, Italy, Latvia, Lithuania, Germany, Poland and the United Kingdom to enable its "multinational and cross-sector participants, from the civilian and military, private and academic sectors" to use modern technologies to produce analysis and research on hostile information operations and NATO strategic messaging. [32]
- The Baltic Center for Media Excellence in Riga was founded in 2015 to train local and national media, and "gather intelligence on regional media trends and skills, as well as research media audiences with a focus on those most vulnerable to propaganda" in eastern Europe.[33] Solvita Denisa-Liepniece, a consultant at the center, said it has helped foster regional journalistic cooperation, improved media best practices and helped identify specific vulnerabilities to disinformation in the region, which Russia uses as a testing ground for its disinformation campaigns.[34]

Cyber Security

- The NATO Cooperative Defense Center of Excellence (CCDCOE) in Tallinn was established in 2008 by Estonia, Latvia, Lithuania, Germany, Italy, Slovakia and Spain "to support our member nations and NATO with unique interdisciplinary expertise in the field of cyber defense research" and with training and exercises in technology, strategy and law.[35] CCDCOE organizes the world's largest and most complex international live-fire cyber defense exercise, Locked Shields, annually.
- The government of Lithuania established the Kaunas Cyber Security Center as a subdivision of the National Cyber Security Center to draw on the expertise of Lithuanian, American, Ukrainian and Georgian cybersecurity experts.[36] To keep NATO one step ahead of the Russians, Kerza said the center in Kaunas allows specialists who deal with Russian cyber operations every day to physically work together to monitor their networks and analyze hostile cyber operations.[37] "We always talk about information sharing, but if you're sharing information about an attack it's already too late," he said.

Section 3: The United States and Europe

The United States must expand cooperation with its central and eastern European partners not only to help bolster their defense capacity but also to help the United States better understand hostile cyber actors' activities and how to counter them. Central and eastern European governments and societies are committed to improving regional cybersecurity and have had to think creatively about becoming more resilient. The United States has partners across central and eastern Europe eager to share their frontline experience in defending against hostile hacking and information attacks on their cyberspace.

That experience dealing directly with hostile cyber actors, combined with U.S. resources and expertise, could vastly improve the security of both the United States and Europe. “If you want to be more secure, you need to do practical work with those who face a real threat from the East,” Kerza said. “If you sit at home thinking that a cyberattack will never reach you, you’ll be wrong.”[38] Meanwhile, Iti Press, the counselor for cyber issues and economic affairs at the Estonian Embassy in Washington, said many Estonian cybersecurity experts have struggled to get access to their U.S. counterparts and emphasized the importance of improving participation in joint cyber exercises taking place in the United States.[39] Sven Sakkov, the former director of ICDS, described U.S. involvement in the NATO CCDCOE in Tallinn, where only one member of the 30 senior staff is an American, as “underwhelming” and urged greater U.S. participation.[40] Likewise, the Latvian defense counselor in Washington, Rolands Heniņš, said, “We are there on the front line facing malign influence for over 30 years, and we have learned our lessons. Use our smart people and knowledge.”[41] Joanna Świątkowska, the former European Cybersecurity Forum official, said the United States and Europe should expand the sharing of threat indicators and early warning information to help harden European and American cyber defenses and present a united front to hostile actors.[42] And Solvita Denisa-Liepniece of the Baltic Center for Media Excellence said the United States could learn from eastern European journalists how hostile states conduct disinformation campaigns and media manipulation.[43]

American-European cooperation in cyberspace will be vital to ensuring the security of the transatlantic community in the face of shared threats from Russia and China. It is highly unlikely that these foes will ever be deterred from launching cyberattacks, but by working together American and European countries can be prepared to manage these attacks as they come and exact a high price on those conducting them. In the coming years, the United States should focus on engaging more with its European partners.

- U.S. Cyber Command should conduct more bilateral and multilateral cyber defense exercises across Europe, with a focus on engaging central and eastern European states and expert communities.
- U.S. Cyber Command should improve existing information-sharing frameworks with its counterparts in central and eastern Europe.
- The U.S. government broadly should bring eastern European cybersecurity and disinformation experts to the United States, where they can engage with, learn from and teach their American counterparts. The U.S. government should also send U.S. experts to work directly with their counterparts in Europe.
- The U.S. government should coordinate strong joint responses with European countries against particularly dangerous or reckless cyber actors such as Russia.
- The U.S. policy community should engage with eastern European officials and experts to learn about the effectiveness of various methods of improving cyber resilience employed in central and eastern Europe.
- The U.S. State Department and Congress should increase dialogue with European governments and the European community to improve and expand ways to name, shame and sanction hostile cyber actors.
- The U.S. government should increase financial assistance for central and eastern European cyber defense and research programs through initiatives such as the Countering Russian Influence Fund.

Endnotes

[1] Fisher S. “Internet of Things Security Risks”. *Avast*. December 9, 2019. https://www.avast.com/c-iot-security-risks; “IOT Connections to Grow 140% to Hit 50 Billion by 2022, as Edge Computing Accelerates ROI.” *Juniper Research*, 2018. https://www.juniperresearch.com/press/iot-connections-to-grow-140pc-to-50-billion-2022

[2] “APT28: At the Center of the Storm- Russia Strategically Evolves Its Cyber Operations,” *FireEye*, https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html

[3] Joanna Świątkowska, former Program Director of the European Cybersecurity Forum, web interview, 19 August 2020.

[4] Rain Ottis, Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, *Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia, January 2008. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[5] Andy Greenberg, “Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers,” *Doubleday*, November 5, 2019; “Could NotPetya’s Tail Be Growing?” *PCS*, *A Verisk Business https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf*

[6] “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace.” *Justice Department*. 19 October 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[7] Zak Doffman. “Russia Unleashes New Weapons In Its ‘Cyber Attack Testing Ground’: Report.” *Forbes*. 5 February 2020. https://www.forbes.com/sites/zakdoffman/2020/02/05/russia-unleashes-new-weapons-in-its-cyberattack-testing-ground-report/?sh=75a37e6f5ce5; Laurens Cerulus. “How Ukraine became a test bed for cyberweaponry.” *Politico*. 14 February 2019. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

[8] Rolands Henins, Defense Counselor, Ministry of Defense of Latvia, Embassy of the Republic of Latvia in the USA, web interview, 19 August 2020

[9] Coats R, “Worldwide Threat Aassesement of the U.S. Intelligence Community” *Senate Select Committee on Intelligence*, 29 January 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[10] Nataliya Bugayova, “How We got Here with Russia: The Kremlin’s Worldview” *The Institute for the Study of War*, March 2019. http://www.understandingwar.org/sites/default/files/ISW%20Report_The%20Kremlin%27s%20Worldview_March%202019.pdf

[11] Mark Galeotti, “Putin’s Hydra: Inside Russia’s Intelligence Services” *European Council on Foreign Relations*, May 11, 2016. https://www.ecfr.eu/page/-/ECFR_169_-_INSIDE_RUSSIAS_INTELLIGENCE_SERVICES_(WEB_AND_PRINT)_2.pdf

[12] Dustin Volz, “Russian hackers tracked Ukrainian artillery units using Android implant:” report *Reuters*, December 2, 2016. https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU; Paulo Shakarian, “The 2008 Russian Cyber-Campaign Against Georgia,” *Military review*, January 1, 2011 https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20111231_art013.pdf

[13] Andy Greenberg. “The NSA Confirms It: Russia Hacked French Election ‘Infrastructure.’” *Wired*. May 9, 2017. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

[14] “Norway blames Russia for cyberattack on parliament.” *BBC*. 13 October 2020. https://www.bbc.com/news/world-europe-54518106; Chris Bing. “Russia-linked hackers impersonate NATO in attempt to ack Romanian government” *Cyberscoop*. 11 May 2017. https://www.cyberscoop.com/dnc-hackers-impersonated-nato-attempt-hack-romanian-government/; “Poland says its repelled a 3rd Russian hacking attack.” *AP*. 13 October 2017. https://apnews.com/article/ae703cec6849457a865a64141554d94e

[15] Nicu Popescu and Stanislav Secrieru, “Hacks, leaks, and disruptions: Russian cyber strategies.” *European Union Institute for Security Studies*. October 2018. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

[16] Veronica Vichova, KremlinWatch at the European Values Center for Security Policy, web interview, 19 August 2020.

[17] Vesselina Pentcheva, “The Tale of Two Chinas: Improving the Dialogue on Chinese Investment in Europe” *Center for European Policy Analysis*, October 2018. https://docs.wixstatic.com/ugd/644196_2c9e1d6d80ed4fb79ac9d03c792a9742.pdf

[18] “Chinese hackers stole at least 1,100 EU diplomatic cables, U.S. cybersecurity firm says” *Associated Press*, December 19, 2018. https://apnews.com/article/0bb42b3bb8fe485cb7bcbbfb7b0be989

[19] Janusz Bugajski, “The West Needs a China Strategy” *Center for European Policy Analysis*, https://www.cepa.org/chinas-eurasian-ambitions

[20] Laurens Cerulus, “China Rebuffs EU warning on hacking hospitals” *Politico*, June 23, 2020 https://www.politico.eu/article/china-rebuffs-eu-warning-hacking-hospitals/; Jennifer Rankin,” EU says China behind ‘huge wave’ of Covid-disinformation” *The Guardian*, 10 June 2020. https://www.theguardian.com/world/2020/jun/10/eu-says-china-behind-huge-wave-covid-19-disinformation-campaign; “Coronavirus: EU strengths action to tackle disinformation” *The European Commission*, June 10, 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006

[21] Michael R. Pompeo, “Welcoming the United Kingdom Decision to Prohibit Huawei from 5G Networks,” *U.S. Department of State*, July 14, 2020. https://www.state.gov/welcoming-the-united-kingdom-decision-to-prohibit-huawei-from-5g-networks/

[22] Edvinas Kerza, former Vice-Minister of National Defense of Lithuania, web interview, 19 August 2020.

[23] “Estonian Defense League- The Kaitseliit- Strong in Defense” *NATO Shape Public Affairs Office*, May 14, 2019. https://shape.nato.int/news-archive/2019/estonian-defence-league-the-kaitseliit-strong-in-defence-;

National Defense Strategy: “Estonia” *Estonian Ministry of Defense*, October 17, 2019. https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf

[24] Olevs Nikers, President of the Baltic Security Foundation, web interview, 19 August 2020

[25] Dan Sabbagh. “Russia-aligned hackers running anti-Nato fake news campaign- report” *The Guardian*. 30 July 2020; https://www.theguardian.com/technology/2020/jul/30/russia-aligned-hackers-running-anti-nato-fake-news-campaign-report-poland-lithuania; “Assessing Russian Activities and Intentions in Recent U.S. Elections” *Intelligence Community Assessment*. 6 January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf

[26] Edvinas Kerza, former Vice-Minister of National Defense of Lithuania, web interview, 19 August 2020.

[27] “Case Study: The world’s first data embassy- Estonia Embracing Innovation in Government: Global Trends” 2018. *OECD*. https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf; Data Embassy. *E-Estonia*. https://e-estonia.com/solutions/e-governance/data-embassy/

[28] Sven Sakkov, Former Director for the International Center for Defense and Security, web interview, 19 August 2020.

[29] “Global Cybersecurity Index 2018.” *ITU Publications*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf; “Global Cybersecurity Index and Cyberwellness Profiles.” 2015. *ITU Publications*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

[30] Edvinas Kerza, former Vice-Minister of National Defense of Lithuania, web interview, 19 August 2020.

[31] Edvinas Kerza, former Vice-Minister of National Defense of Lithuania, web interview, 19 August 2020.

[32] “About Us” *NATO Stratcom Center of Excellence*. https://www.stratcomcoe.org/about-us;

[33] “About” *Baltic Center for Media Excellence*. https://bcme.eu/en/about/

[34] Dr. Solvita Denisa-Liepniece, Baltic Center for Media Excellence, web interview, 19 August 2020.

[35] “About Us” *NATO Cooperative Cyber Defense Center of Excellence*. https://ccdcoe.org/about-us/

[36] “Lithuanian president visits cybersecurity center in Kaunas” 15 January 2020, *Honorary Consul of the Republic of Lithuania in Bangkok*. http://www.lithuaniahonoraryconsulinbangkok.com/news-evnts/news/4167-lithuanian-president-visits-cybersecurity-center-in-kaunas.html; Saulius Jakucionis. “Lithuania to bolster cybersecurity -early warning system, additional cybersecurity center” *LRT News*. 07 March, 2019. https://www.lrt.lt/en/news-in-english/19/1075107/lithuania-to-bolster-cybersecurity-early-warning-system-additional-cybersecurity-center

[37] Edvinas Kerza, former Vice-Minister of National Defense of Lithuania, web interview, 19 August 2020.

[38] Edvinas Kerza, former Vice-Minister of National Defense of Lithuania, web interview, 19 August 2020.

39 Mrs. Iti Press, Counsellor for Cyber Issues and Economic Affairs, Embassy of the Republic of Estonia, web interview, 10 September 2020.

40 Sven Sakkov, Former Director for the International Center for Defense and Security, web interview, 19 August 2020.

41 Rolands Henins, Defense Counselor, Ministry of Defense of Latvia, Embassy of the Republic of Latvia in the USA, web interview, 19 August 2020

42 Joanna Świątkowska, former Program Director of the European Cybersecurity Forum, web interview, 19 August 2020.

43 Dr. Solvita Denisa-Liepniece, Baltic Center for Media Excellence, web interview, 19 August 2020.

CEPA

Center for European Policy Analysis
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004
info@cepa.org | www.cepa.org