Atlantic Council

Alliance Power for Cybersecurity

Kenneth Geers

ABSTRACT

There is only one Internet, and it is fragile. In this new global domain, nation-states are surprisingly limited in what they can do to defend against international cybercrime, espionage, terror, and war. Beyond pure technical expertise, the most effective cybersecurity strategy for any government is to collaborate with allies. For democracies, the only credible political and military alliances are the European Union (EU) and NATO, whose member states comprise dozens of like-minded nations and hundreds of first-class network security, law enforcement, and intelligence agencies. Together, they constitute the world's only cyber superpower.

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The Scowcroft Center's Transatlantic Security Initiative brings together top policymakers, government and military officials, business leaders, and experts from Europe and North America to share insights, strengthen cooperation, and develop innovative approaches to the key challenges facing NATO and the transatlantic community. This publication was produced in partnership with the Lithuanian Ministry of National Defense under the auspices of a project focused on defense and deterrence in the Baltic Sea region.

The Cyber Statecraft Initiative works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

ISBN-13: 978-1-61977-097-3

Cover photo credit: Gerd Altmann.

CONTENTS

Cyber defense exercise, organized and run by NATO's Allied Command Transformation, 2016.
Photo credit: NIC Edouard Bocquet/NATO.

FOREWORD

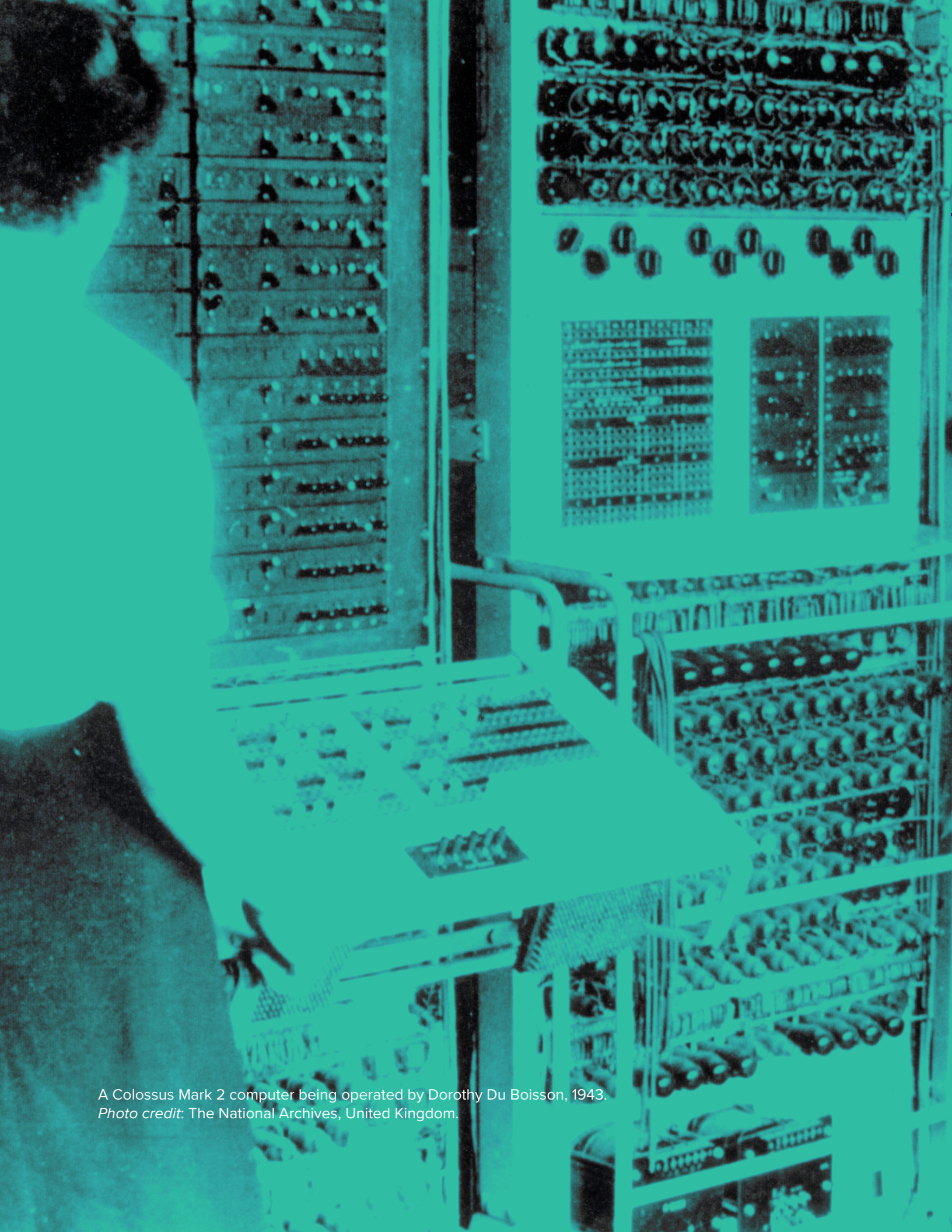
There is one Internet today but that is not the case without collective effort and purposeful will. The imposition of hard physical borders and barriers to movement amidst the world's response to the novel coronavirus remind us of the fragile trust with which data moves across these same borders. While fiber lines and radio waves may criss-cross the globe unconstrained by more than physics, their owners are subject to law and political force. How fast will the newfound limits imposed by COVID-19 on free movement of trade and people fade? How many of those same limits will be extended to cyberspace and the movement of information?

Cybersecurity amidst the coronavirus has taken on added urgency and focus as the introduction of remote work across multiple continents has laid bare the terrific dependence of modern society on the Internet. In our reliance on video conferencing and Voice over Internet Protocol (VOIP), cloud productivity software, and streaming video, we are experiencing a collective revitalization of digital spaces both professional and personal. The security challenges posed by this frequency and depth of engagement across the Internet presents renewed opportunities for malign actors, be they criminals or nation-states, to abuse the new realities of digital collaboration. Working collectively and effectively in defense of the Internet is as difficult as grasping the technical capabilities needed to address the actual security threats.

Maintenance of the Internet's value requires constant temperance from all who use, design for, commit to, and maintain it. While the current global health crisis tempts the imposition of barriers to ideas and community, it must not be allowed to undermine the Internet. The United States and its allies have a monumental task to provide sober Internet governance amidst this crisis. This report's recommendations for collective action to identify, investigate, and mitigate harms to the Internet will increase our collective technical resilience and guard against a dissolution of our greater political community.

Trey Herr
Director, Cyber Statecraft Initiative,
Scowcroft Center for Strategy and Security,
Atlantic Council

Christopher Skaluba
Director, Transatlantic Security Initiative,
Scowcroft Center for Strategy and Security,
Atlantic Council



A Colossus Mark 2 computer being operated by Dorothy Du Boisson, 1943.
Photo credit: The National Archives, United Kingdom.

1. INTRODUCTION
THERE IS ONLY ONE INTERNET

On July 26, 1939, on the eve of World War II, three Polish cryptanalysts—Marian Rejewski, Jerzy Różycki, and Henryk Zygalski—began to share previously classified code-breaking techniques for the German Enigma device with French and British intelligence. By the end of the war, the Allied effort to decrypt Nazi communications, known in Britain as Project Ultra, was so successful that it may have significantly shortened the conflict. Harry Hinsley, a cryptanalyst and historian of Britain's Bletchley Park cryptologic group, wrote that without the knowledge gained from Ultra, Operation Overlord (the Allied invasion of France) would likely have been deferred for two years—until 1946.[1]

Nearly eight decades after the end of World War II, the astonishing power of modern information technology (IT) has transformed human civilization—from personal relationships to government services. With artificial intelligence (AI), quantum computing, biohacking, and more just over the horizon, our children will live in an IT-enabled world that we can scarcely imagine. On balance, we have gained far more than we have lost. No one in her right mind would trade world-class free education[2] for the slightest reduction in cyberattacks.

So why all the fuss over cybersecurity? Two reasons: first, all digital information is vulnerable to theft, denial, or manipulation; second, every computer, no matter how sensitive, is somehow connected to the Internet, and exposed to hackers. What's the worst that could happen? In theory, an attacker could try to ignite Armageddon by impersonating the US president, acquiring nuclear launch codes, or fooling the White House into thinking that a foreign nuclear attack had begun.[3] These are unlikely scenarios, but as we hope for the best, we must prepare for the worst.

Some challenges, such as global warming, or the coronavirus outbreak, are inherently international. They are so vast that no nation can solve them alone. Cybersecurity falls into that category. Today, the 191 member states of the United Nations share but one Internet (made of computer hardware and software), and one cyberspace (the Internet's connection to humanity). Every government is now trying to defend its national sovereignty in cyberspace—and failing.

Computer network operations offer attackers three crucial advantages: easy acquisition, sharp asymmetry, and murky attribution (although the offense-defense balance is constantly shifting). First, digital tools and tactics are widely available; a belligerent program can be hidden in plain sight, as cyberattack and defense are essentially the same discipline. Second, the investment costs for attack, when compared to defense and mitigation, can be pennies on the dollar; even teenagers have caused millions in corporate losses.[4] Third, the bad guys can be hard to find because they hijack third-party computers, and route attacks through the international, maze-like architecture of the Internet.[5]

None of this is new to most governments. Before the digital age, law enforcement tapped telephone lines,

1 Andrew Lycett, "Breaking Germany's Enigma Code," BBC, Last updated February 17, 2011, http://www.bbc.co.uk/history/worldwars/wwtwo/enigma_01.shtml.

2 Clive Thompson, "How Khan Academy Is Changing the Rules of Education," *Wired*, July 5, 2011, https://www.wired.com/2011/07/ff_khan/.

3 After viewing the movie *WarGames*, then-President Ronald Reagan is reported to have asked John Vessey, the chairman of the Joint Chiefs of Staff, if something like this could really happen. One week later, according to the book *Dark Territory,* General Vessey returned with a startling answer: "Mr. President, the problem is much worse than you think." Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, (New York: Simon & Schuster, 2016), 1–2.

4 In 2001, a teenager named "MafiaBoy" caused millions in corporate damages with a simple denial-of-service (DoS) attack. See: Dan Verton, *The Hacker Diaries: Confessions of Teenage Hackers* (New York: McGraw-Hill/Osborne, 2002).

5 David A. Wheeler and Gregory N. Larsen, "Techniques for Cyber Attack Attribution," Institute for Defense Analyses, October 2003, https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf. Some aspects of this problem have changed little since 2003, when this paper nicely described both the attribution problem as well as strategies to overcome it.

intentionally misdirected calls, and eavesdropped on conversations. In the 1970s, some of the first citizen hackers (called phreakers) whistled the signal frequency at which telephone numbers were dialed to make calls for free.[6] Universal machines can have universal vulnerabilities. As computers escaped laboratories and invaded our businesses and homes, functionality and connectivity usually outpaced security—including within our national critical infrastructures. As a consequence, everything from electricity to elections is now exposed to some level of Internet-based crime, espionage, terrorism, and warfare. Therefore, at least within the national security community, some networks began to implement cyber defense measures by the 1960s.[7] In the following decade (while Leonid Brezhnev was still in charge of the Kremlin), national security strategists were already dissecting the information wars of the future, this time, at the level of bits and bytes.[8]

Nonetheless, it would take another generation for public awareness to catch up. In 1989, Clifford Stoll published *The Cuckoo's Egg*, the astonishing tale of how a young astronomer working as a systems manager at Lawrence Berkeley Lab chased a $0.75 accounting error in California all the way back to the KGB (the Soviet State Security Committee) in Moscow.[9] In 1997, Bill Clinton set up the President's Commission on Critical Infrastructure Protection (PCCIP). Its final report, *Critical Foundations: Protecting America's Infrastructures,* identified eight economic sectors of "strategic security value: telecommunications, electric power, gas and oil, water, transportation, banking and finance, emergency services, and government continuity." Further, PCCIP recognized that each of these infrastructures was managed by, and dependent on, IT systems that had "pervasive" vulnerabilities threatened by a "wide spectrum" of adversaries.[10]

Today, there are so many stories of hackers and computer compromises in the news that cybersecurity is intuitively a national-level challenge, from kindergarten to Congress. Less obvious, however, is the fact that no nation—not even the United States, Russia, or China—can successfully address this challenge alone. There is only one Internet, and one cyberspace, enveloping the whole of planet Earth. Individuals, enterprises, and nations isolate themselves from its benefits at their own risk. Cybersecurity is therefore "an international problem that requires an international solution,"[11] even while myriad geopolitical rifts are likely to endure for the foreseeable future. As a result, the best place to begin this journey is with political and military allies—specifically, the democratic nations of the European Union (EU) and NATO.

---

6 Umesh Hodeghatta Rao and Umesha Nayak, "History of Computer Security," *The InfoSec Handbook* (Berkeley, California: Apress, 2014), https://link.springer.com/chapter/10.1007/978-1-4302-6383-8_2.

7 In the mid-1960s, the US Advanced Research Projects Agency (ARPA) contracted the Massachusetts Institute of Technology (MIT) to build the Multics (Multiplexed Information and Computing Service) operating system, which was designed with military-grade security in mind, to protect computer users from both external attacks and each other. See: Eugene H. Spafford, "Unix and Security: The Influences of History," Purdue University paper, 1991, https://docs.lib.purdue.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1924&context=cstech.

8 Thomas P. Rona, "Weapon Systems and Information War," Boeing Corp., July, 1976, https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf.

9 Not only is this the first book on nation-state hacking, it is also the best. Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Doubleday, 1989), 326.

10 "Critical Foundations: Protecting America's Infrastructures," a report of the President's Commission on Critical Infrastructure Protection, October 1997, https://fas.org/sgp/library/pccip.pdf.

11 Kenneth Geers, "Kosovo, Cyber Security, and Conflict Resolution," paper presented at the Friedrich Ebert Stiftung conference, "Current Security Challenges for the Western Balkan region," November 19–21 2014, Prishtina, Kosovo, http://www.2501research.com/new-blog/2014/11/25/kosovo-conflict-resolution.

2. #CYBERWAR
INTERNATIONAL CONFLICT IN CYBERSPACE

IT is a Swiss Army knife. It is now used for anything and everything, everywhere. To a large degree, this is what makes cyber defense so hard: Every cyberattack has some unique characteristics, and it is hard to know where (or how) hackers will strike next. It is always worth remembering, however, that a computer network operation is not an end in itself, but a means to some other criminal, political, intelligence, or military goal.

The number of capable cyber actors is always growing: Criminal syndicates are old hands; private companies now offer hacking as a service (including "hack-back" to help identify intruders);[12] and terrorists, who have long used the World Wide Web for propaganda, recruitment, and fundraising, have lacked sufficient infrastructure to pose a strategic hacker threat, but will always remain a dangerous wild card.[13] At the government level, intelligence agencies leverage computer hacking to steal, block, and manipulate information in support of a wide array of perceived national security goals. This practice extends to countries with poor human rights records, little respect for the rule of law, and national strategies that run counter to the democratic norms of the EU and NATO.

During the Cold War, the primary information security threat emanated from the Soviet Union, but today, via the global Internet, many more nations are active in this geostrategic space, including China, Iran, and North Korea. China has pioneered and now exported the concept of a "Great Firewall" of digital censorship, surveillance, and sovereignty.[14] The United States and Iran have been engaged in cyber battles, from underground bunkers in Iran to the Nasdaq Stock Exchange in New York City, for years.[15] And North Korean leader Kim Jong Un has called cyber warfare an "all-purpose sword" that, along with nuclear weapons and missiles, gives his military a "ruthless striking capability."[16]

Nevertheless, the single largest body of cyberattack literature to date has detailed incidents that have occurred just across EU and NATO borders, many of which should have been seen as harbingers of cyberattacks elsewhere. From its advent in the early 1990s, the World Wide Web revolutionized the delivery of propaganda and psychological operations (PSYOP). Russia fought two wars in Chechnya, where battles for traditional terrain quickly turned into battles for digital terrain.[17] Chechen rebels found that the Internet was perfect for networking and fundraising,[18] which led to the hacking of websites such as kavkaz.org (likely by

12 Nicholas Schmidle, "The Digital Vigilantes Who Hack Back," *New Yorker*, April 30, 2018, accessed September 4, 2019, https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

13 Irving Lachow and Cortney Richardson, "Terrorist Use of the Internet: The Real Story," *Joint Force Quarterly* (JFQ), National Defense University Press, 45 (2007), https://apps.dtic.mil/dtic/tr/fulltext/u2/a518156.pdf.

14 Danny O'Brien, "China's Global Reach: Surveillance and Censorship Beyond the Great Firewall," Electronic Frontier Foundation, October 10, 2019, https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall.

15 Jacquelyn Schneider, "It's Time to Calibrate Fears of a Cyberwar with Iran," *New York Times*, January 7, 2020, https://www.nytimes.com/2020/01/07/opinion/iran-cyber-attack-hacking.html.

16 Kong Ji Young, Kim Kyoung Gon, and Lim Jong In, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," Eleventh International Conference on Cyber Conflict, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Publications, Tallinn, 2019, https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf.

17 Paul Goble, "Russia: Analysis from Washington—A Real Battle on the Virtual Front," Radio Free Europe/Radio Liberty, October 9, 1999, https://www.rferl.org/a/1092360.html.

18 The number to a bank account in California was put online so that anyone in the world could donate to the cause. See: Timothy L. Thomas, "Information Warfare in the Second (1999–Present) Chechen War: Motivator for Military Reform?," first published in *Russian Military Reform 1992–2002*, Frank Cass Publishers (2003): 209–233; and posted online by All Partners Access Network (APAN), https://community.apan.org/cfs-file/__key/docpreview-s/00-00-08-52-36/2002_2D00_01_2D00_01-Information-Warfare-in-the-Second-_2800_1999_2D00_Present_2900_-Chechen-War-_2800_Thomas_2900_.pdf.

Moscow, and despite its being hosted in the United States).[19] The Kremlin announced "centralized military censorship" in the "North Caucasus," and Vladimir Putin (then Russia's prime minister) announced that "we surrendered this [Internet] terrain some time ago . . . but now we are entering the game again."[20]

In 1999, as NATO went to war with Serbia over the fate of Kosovo, the Alliance naturally sought to leverage its relatively more modern military arsenal. However, computer hackers operating on behalf of Serbia, with historically provocative names like the "Black Hand 2.0"[21] retaliated in novel ways, inundating NATO computer networks[22] with denial-of-service (DoS) attacks and virus-infected email.[23] Bogus traffic choked NATO's email server and rendered its public affairs website inoperable. NATO spokesman Jamie Shea said hackers in Belgrade employed a junk data "bombardment strategy." As NATO frantically defended its computer infrastructure, the malicious data streams (which initially came from Serbia) began to emanate from all over the world.[24] In Washington, hackers defaced the White House website.[25] Western information operations were tightly veiled in secrecy, but some analysts believe that one U.S. Joint Task Force had overseen the first-ever allied cyber war.[26`]

For many national security observers, the first time that the concept of cyber war[27] moved from the realm of science fiction to reality was in Estonia in 2007. The tiny Baltic nation was in a serious diplomatic row with Moscow over the relocation of a Soviet World War II monument (the *Bronze Soldier*) that had stood in downtown Tallinn since 1947. To Estonians, the statue was a constant reminder of seven decades of Soviet occupation; to the Kremlin, it represented both 20th-century wartime sacrifices and 21st-century propaganda points. When Estonia defied Russia and began the move, a barrage of cyberattacks targeted Estonian government, banking, and media websites over the course of several weeks. These included both easy-to-fix web defacements[28] and more alarming incidents such as the disabling of a government router. In the end, "Web War One"[29] was likely more experiment than assault. However, Estonia offers a compelling case study to this day, in part because it had already gone further than most nations in digitizing its economy. One distributed denial-of-service (DDoS) attack successfully knocked Estonian banks off-line for a few hours. In that light, when does a network security incident become a national security incident?[30]

In fact, the cyberattack on Estonia quickly became a point of discussion at the highest level of international relations. Estonian President Toomas

19 According to a Reuters article, two sites (www.kavkaz.org and www.chechenpress.com) "collapsed under a barrage of attacks from computer hackers just after Russian troops stormed a Moscow theater killing forty-one armed rebels and 128 of the hostages they had been holding there." See: Oliver Bullough, "Russians Wage Cyber War on Chechen Websites," Reuters, November 15, 2002, http://archive.cert.uni-stuttgart.de/isn/2002/11/msg00064.html.

20 Goble, "Russia: Analysis."

21 Named after the Pan-Slavic secret society that helped to start World War I.

22 "Yugoslavia: Serb Hackers Reportedly Disrupt US Military Computer," Bosnian Serb News Agency SRNA, March 28, 1999, as reported by BBC Monitoring Service, March 30, 1999.

23 "Evidence Mounts of Pro-Serbian Internet Attack on NATO Countries," mi2g, April 17, 1999 http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/170499.php.

24 Dan Verton, "Serbs Launch Cyberattack on NATO," Federal Computer Week, April 4, 1999, https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx?m=2.

25 Kenneth Geers, "Hacking in a Foreign Language: A Network Security Guide to Russia," presented at the Def Con hackers convention, 2005, https://www.defcon.org/images/defcon-13/dc13-presentations/dc-13-geers.pdf.

26 Bob Brewin, "Kosovo Ushered in Cyberwar," Federal Computer Week, September 27, 1999, https://fcw.com/articles/1999/09/27/kosovo-ushered-in-cyberwar.aspx?m=2.

27 Cyber war is a subjective concept, but here I mean the use by a nation-state of a computer network operation to achieve something more than a tactical national security objective.

28 One defacement on the Estonian prime minister's website apologized for having moved the statue and promised to put it back.

29 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/.

30 Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," *SC Magazine*, August 27, 2008, https://www.scmagazine.com/home/opinions/cyberspace-and-the-changing-nature-of-warfare/.

Ilves received an invitation to the White House,[31] in part to discuss whether a future cyberattack (which did not employ conventional weapons systems or result in the immediate loss of life) could be considered an armed attack. The NATO alliance, which Estonia joined in 2004, is built on the foundation of collective defense. NATO's Article Five states that "an armed attack against one or more [member countries] in Europe or North America shall be considered an attack against them all."[32] Suleyman Anil, then head of NATO Cyber Defence, said "Estonia was the first time . . . [we saw] possible involvement of state agencies; that the cyber attack can bring down a complete national service, banking, [and] media."[33] As a result, NATO decided to move quickly: Whereas previous NATO Strategic Concepts had made no mention of computers, the Internet, cyberspace, or hackers,[34] by 2010 cyberattacks were placed alongside terrorism and ballistic missiles as primary threats to the Alliance in these documents outlining fundamental security tasks.[35]

Ultimately, the concept of cyber war does not mean anything absent a wider context. Electronic warfare and special operations are merely unique facets of war, just like diplomacy and espionage are subordinate to international (and domestic) politics. Nonetheless, it is clear that militaries and intelligence agencies are employing computer network operations with increasing frequency and effect. Today, most countries have been on the receiving end of a cyberattack. Since Estonia's case, there are many prominent examples on NATO's borders: In 2008, Russia used cyberattacks to facilitate a military invasion of Georgia.[36] In 2009, during a domestic political crisis, a DoS attack knocked the entire nation of Kyrgyzstan off-line.[37] In 2014, a drone trailing a nationalist Albanian flag was flown through a football stadium in Belgrade, sparking ethnic tensions, a diplomatic row between Serbia and Albania,[38] and online battles between partisan hackers.[39] In 2016, Russian military intelligence ran cyber operations, including the staged release of official documents stolen through computer intrusions, to interfere in the US presidential election.[40] In 2018, hackers allegedly based in Russia launched a cyberattack from a Lithuanian television station that simultaneously disseminated both fake news and malware.[41] During this same time period, there have been so many examples of cyberattacks in Ukraine that they are analyzed in a separate section, below.

---

31 "President Bush Welcomes President Ilves of Estonia to the White House," Office of the Press Secretary, White House, June 25, 2007, https://georgewbush-whitehouse.archives.gov/news/releases/2007/06/20070625.html;
I also received a one-way ticket to Tallinn to help build the NATO Cyber Defence Centre of Excellence, as its first international researcher: "About us," the NATO Cooperative Cyber Defence, https://ccdcoe.org/about-us/.

32 "The North Atlantic Treaty," NATO, Washington, DC, April 4, 1949; last updated April 10, 2019, https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

33 Frank Gardner, "NATO's Cyber Defence Warriors," BBC News, February 3, 2009, http://news.bbc.co.uk/2/hi/europe/7851292.stm.

34 "Strategic Concepts," NATO, last updated June 12, 2018, https://www.nato.int/cps/en/natohq/topics_56626.htm.

35 "NATO 2020: Assured Security; Dynamic Engagement," NATO, May 17, 2010, https://www.nato.int/cps/en/natolive/official_texts_63654.htm.

36 Paulo Shakarian, "The 2008 Russian Cyber Campaign against Georgia," *Military Review*, Army University Press (November–December 2011), https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20111231_art013.pdf.

37 Gregg Keizer, "Russian 'Cyber Militia' Knocks Kyrgyzstan Offline," Computerworld, January 28, 2009, https://www.networkworld.com/article/2262155/russian--cyber-militia--knocks-kyrgyzstan-offline.html.

38 Dan Bilefsky, "Drone Stunt at Belgrade Soccer Match Stirs Ethnic Tensions," *New York Times*, October 17, 2014, https://www.nytimes.com/2014/10/18/world/europe/drone-stunt-at-belgrade-soccer-match-stirs-ethnic-tensions.html.

39 Geers, "Kosovo, Cyber Security, and Conflict Resolution."

40 United States v. Netyksho, Antonov, Badin, Yermakov, Lukashev, Morgachev, Kozachek, Yershov, Malyshev, Osadchuk, Potemkin, and Kovalev, 1:18-cr-215 (D.D.C. 2018) (indictment): 29, https://www.justice.gov/file/1080281/download.

41 Dalia Bankauskaitė and Simas Čelutka, "Cyberattacks in Lithuania: The New Normal," StopFake.org, May 6, 2018, https://www.stopfake.org/en/cyberattacks-in-lithuania-the-new-normal/.

3. COLLECTIVE DEFENSE
COLLABORATION IN CHAOS

Allied leaders signed the Atlantic Charter on August 14, 1941, outlining their vision for postwar international relations that would include self-determination, interstate cooperation, disarmament, and a higher standard of living for all.[42] In the Internet age, these democratic ideals have not changed. However, national security threats including crime, espionage, terrorism, and war now occur not only in physical space but also in the international domain of cyberspace, where any single government's sovereignty and defenses are quite limited. As a consequence, many hacker tools and tactics are best countered via international collaboration in network security and law enforcement.

That is easier said than done: I used to participate in international cyber investigations, and success stories are not written every day.[43] Further, there is a huge gap between strategic vision and tactical reality. Modern IT is complex, ubiquitous, rapidly evolving, shrinking in size, and often encrypted. National decision makers are mystified by the prosaic Internet use of their grandchildren. Political pressures exacerbate these challenges: Law enforcement must conduct domestic surveillance;[44] intelligence services must conduct foreign espionage;[45] but citizens must also have rule of law, and a guaranteed level of data privacy.

At the enterprise level, there are analogous tensions. Security often takes a backseat to functionality and usability. For example, the current "language" of computer networks is Internet Protocol version 4 (IPv4), which has "been in use since 1983, and suffers from many shortcomings, including size, speed, and security.[46] Its successor, IPv6, is larger, faster, and more secure—but the world has been slow to adopt it. Why? For the same reason that humans are slow to learn a new language: IPv6 takes a lot of time and effort to master, and humans prefer simply to get by on what they already know. Countless deadlines have been missed, and still no one seems sure that it's really worth the investment.[47]

These cybersecurity challenges may be with us for many years to come. Therefore, nation-states are integrating cyber defense—and cyberattack—into everything they do. In 2010, the United States was the first nation to create a military command devoted entirely to cyber war,[48] but since then, all major powers have followed suit.[49] Cyberspace is now home to thousands of nation-state computer

42 "1941: The Atlantic Charter," United Nations website, https://www.un.org/en/sections/history-united-nations-charter/1941-atlantic-charter/index.html.

43 Cyber defense analysts are typically overwhelmed by the variety and volume of malicious code they see, as well as the billions of foreign Internet Protocol (IP) addresses from which it emanates. I know this firsthand, having worked cyber investigations as far back as the USS Cole bombing in 2000, as an analyst at the Naval Criminal Investigative Service (NCIS). Successful investigations are rarely possible without international partnerships, which is why the Federal Bureau of Investigation (FBI) has posted hundreds of cyber agents overseas.

44 For an overview of what the FBI sees as its current cyber responsibilities, see: "Cyber Crime," FBI, https://www.fbi.gov/investigate/cyber.

45 Sun Tzu devoted an entire chapter of *The Art of War* to espionage, referring to a leader who obstinately remains ignorant of enemy plans as "inhuman." See chapter XIII, "The Use of Spies," in *The Art of War*, trans. Lionel Giles, http://classics.mit.edu/Tzu/artwar.html.

46 This choice may be analogous to the purchase of an electric car. It seems the right thing to do, but buyers fear unfamiliarity and a possible lack of infrastructure. See: Kenneth Geers and Alexander Eisen, "IPv6: World Update," ICIW 2007: Second International Conference on i-Warfare and Security, Naval Postgraduate School, Monterey, California, 2007, https://simson.net/ref/2007/iciw07-cd.pdf.

47 David Holder, "Blockers to IPv6 Adoption," RIPE (Réseaux IP Européens), June, 7, 2018, https://labs.ripe.net/Members/david_holder/blockers-to-ipv6-adoption.

48 Cheryl Pellerin, "Lynn: Cyberspace Is the New Domain of Warfare," American Forces Press Service, October 19, 2010, https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/884164/lynn-cyberspace-is-new-domain-of-warfare/.

49 According to the Council on Foreign Relations Digital and Cyberspace Policy Program's "Cyber Operations Tracker," twenty-five countries are currently suspected of sponsoring cyber operations, (https://www.cfr.org/interactive/cyber-operations), but I think that number is far too low, as all nation-states today must be able to hack a remote computer if and when the need arises.

network operations that criss-cross the globe in every direction, every day. In many cases, their legality is dubious,[50] but at the dawn of cyber conflict, international norms are nascent and volatile.[51] Major attacks like Stuxnet[52] and NotPetya[53] are constantly testing the waters and pushing the envelope.

The current "laws of war" were written on the assumption that a border would be crossed, or that someone would die. With the relatively bloodless nature of cyberattacks (so far), the "attribution problem" (knowing the true source of an attack in a timely fashion),[54] and overlapping national sovereignties in cyberspace combine to make deterrence and retaliation a challenge. Even national-level cybersecurity programs such as China's Golden Shield Project, Russia's SORM,[55] and the USA PATRIOT Act, have been more successful at generating human rights concerns than preventing cyberattacks, due to their "Big Brother"-class surveillance capabilities. Strategy here is tricky, because if a government exercises too much control (as in North Korea), the advantages of IT disappear, the economy withers, and citizens will eventually revolt.

Our inability to defend against cyberattacks will inevitably lead to arms control initiatives for cyberspace. "One possible model is the 1997 Chemical Weapons Convention (CWC), which compels signatories to destroy CW stockpiles, forbids them from producing any more, and gives practical aid to its members in the form of advocacy and the peaceful advancement of science."[56] International cyber diplomacy may not, however, make the political or technical challenges any easier. "Malicious code" is hard to define, and therefore to prohibit. Computer code also can be stored (and encrypted) almost anywhere, which makes an effective inspection regime hard to imagine.[57]

More likely it will be some kind of digital nonaggression pact. In 1998, the Russian government sponsored UN Resolution 53/70, which condemned the abuse of Information and Communication Technology by criminals and terrorists.[58] While many other nations (including the United States) eventually signed this document, the UN remains riven by divisive, age-old geopolitics that usually prevent international agreements from becoming globally-adopted agreements. There is a fundamental difference between a liberal democratic approach to problem-solving and that of authoritarian regimes. In this case, Western observers often fear that Russian and Chinese cybersecurity proposals are mere covers for unscrupulous political opportunism.[59]

Ultimately, what East and West must understand is that there is only one Internet. Modern IT—to include computers, code, operating systems, applications, and network protocols—is inherently international. All attempts at digital isolationism will end, sooner or later. For example, the Internet's technical aspects were once managed by the US

50 The best reading on this subject is often found at the University of Toronto's Citizen Lab: https://citizenlab.ca/. Separately, a legal example includes the NATO-sponsored Tallinn Manual, which examines international law in the context of cyber warfare, focuses primarily on armed conflict, and shies away from saying too much about cyber intervention below the threshold of armed attack—which is where most computer network operations currently lie; see Dieter Fleck, "Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual," *Journal of Conflict and Security Law*, (2013), https://academic.oup.com/jcsl/article-abstract/18/2/331/821668.

51 For the past decade, Moscow State University and MIT have held annual conferences devoted to government, academic, and private-sector perspectives on the development of international norms for cyberspace.

52 David Sanger, "Iran Fights Malware Attacking Computers," *New York Times*, September 25, 2010, https://www.nytimes.com/2010/09/26/world/middleeast/26iran.html.

53 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

54 Computer network operations are typically routed through unwitting third parties, via compromised proxy computers that serve to obscure the trail of an attacker. This dynamic facilitates short-term cyberattacks but has a corrosive effect on the long-term integrity of the Internet; in one sense, it makes a cyberattack against anyone a cyberattack against everyone.

55 *Система Оперативно-Розыскных Мероприятий* or "System for Operative Investigative Activities."

56 Geers, "Kosovo, Cyber Security, and Conflict Resolution."

57 Kenneth Geers, "Cyber Weapons Convention," *Computer Law and Security Review* (2010), https://www.sciencedirect.com/science/article/pii/S0267364910001081.

58 UN General Assembly, Resolution 53/70, "Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/53/70 (January 4, 1999), https://digitallibrary.un.org/record/265311.

59 John Markoff and Andrew Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace," *New York Times*, June 27, 2009, https://www.nytimes.com/2009/06/28/world/28cyber.html.

Department of Defense; but since 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) has performed this mission, leveraging an international, multistakeholder model.[60] Today, most international bodies have a cyber mission. The Organization for Security and Co-operation in Europe (OSCE)—with fifty-six member nations extending from North America to Central Asia—holds regular cybersecurity workshops, and has published sixteen signed Confidence Building Measures (CBM) designed to promote security and stability in cyberspace.[61]

No fewer than twenty-five nations now staff the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, which publishes a free library of cybersecurity research, holds the annual International Conference on Cyber Conflict (CyCon), and manages the world's largest cyber defense exercise "Locked Shields."[62] Small nations can punch well above their weight in the asymmetric world of IT. Elsewhere in the Baltics, Latvia has built the NATO Strategic Communications Centre of Excellence,[63] and Lithuania has created the region's newest showpiece, the National Cyber Security Centre, where all practical aspects of cyber defense are housed under one roof, including research and development, analysis, and incident response.[64] The Centre manufactures its own secure hardware on-site and is working to incorporate securely developed software into critical cyber infrastructure such as systems involved in elections in Lithuania.[65] The Centre is also focused on training with allies, passing on lessons-learned from Lithuania's experience confronting frequent cyber incidents. In fact, Lithuania was already well-known for its cyber-savvy citizenry, dubbed the "elves," who for years have battled Russian trolls waging disinformation campaigns on the World Wide Web.[66]

Ideally, the goals of all such international cybersecurity initiatives should be global in scope, because even the great powers—despite their increasing tactical cyber prowess—are quite limited in what they can achieve at the strategic level. However, traditional geopolitical rifts, as well as the dynamic and unpredictable nature of IT, suggest that we are unlikely to see near-term breakthroughs on a global scale, but rather within the context of alliances. In fact, at this time, the only conceivable cyber superpower is an international alliance, made possible through political and practical collaboration on network security, law enforcement, counterintelligence, and foreign intelligence.

This process has already begun and is not limited to the democratic nations of the EU and NATO. The Shanghai Cooperation Organization (SCO), composed of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan, is the largest bloc in terms of territory and population. In 2009, the SCO signed an agreement on "Cooperation in the Field of International Information Security."[67] In 2011, it published the "International Code of Conduct for Information Security."[68] Again, from a Western perspective, these efforts are not without merit; however, liberal democracies are rightly suspicious that authoritarian regimes are not primarily

60 That said, ICANN only makes sure that information, in the form of data "packets," gets from point A to point B on the Internet; it does not control access, police content, or stop cyberattacks. In theory, the US government has the right to veto fundamental changes to the system, but in practice ICANN operates independently. For example, see: Declan McCullagh, "No Support for U.S. Proposal for Domain Name Veto," CNET News, February 28, 2011, https://www.cnet.com/news/no-support-for-u-s-proposal-for-domain-name-veto/.

61 "Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," Organization for Security and Co-operation in Europe, March 10, 2016, https://www.osce.org/pc/227281?download=true.

62 NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, https://ccdcoe.org/.

63 NATO Strategic Communications Centre of Excellence, Riga, Latvia, https://www.stratcomcoe.org/.

64 All NATO allies and partner countries are invited to work in this center in both security monitoring and incident response roles. National Cyber Security Centre, Vilnius, Lithuania, https://www.nksc.lt/en/.

65 Jen Judson, "A necessary rise: Lithuania bolsters its cybersecurity, catching the attention of other nations," *Fifth Domain*, July 16, 2019, https://www.fifthdomain.com/smr/a-modern-nato/2019/07/15/a-necessary-rise-lithuania-bolsters-its-cybersecurity-catching-the-attention-of-other-nations/

66 Kim Sengupta, "Meet the Elves, Lithuania's Digital Citizen Army Confronting Russian Trolls," Independent, July 17, 2019, https://www.independent.co.uk/news/world/europe/lithuania-elves-russia-election-tampering-online-cyber-crime-hackers-kremlin-a9008931.html.

67 "Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization," SCO, http://eng.sectsco.org/load/207508/.

68 "International Code of Conduct for Information Security," annex to the letter dated September 12, 2011, from the permanent representatives of China, Russia, Tajikistan and Uzbekistan to the United Nations, addressed to the Secretary-General, A/66/359, September 14, 2011, https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/UN-110912-CodeOfConduct_0-1.pdf.

The Ministry of National Defense of Lithuania. The ministry is responsible for setting Lithuanian cybersecurity policy. *Photo credit*: Bernt Rostad/Wikimedia Commons.

interested in cybersecurity per se, but seek to use the power of IT above all as a surveillance system in a way that ignores human rights and serves to keep autocrats in power.[69]

The political alliance with the greatest achievements in information security is the EU, with twenty-eight sovereign member states, more than five-hundred million residents, and an economy nearly the size of the US economy.[70] In 2001, the EU created the Council of Europe's Convention on Cybercrime (aka the Budapest Convention), which is the only binding international agreement for cybersecurity, and an archetypal template for all countries to use domestically, now signed by over fifty nations from around the world. Today, the EU has a robust framework for electronic signatures, online services, spam filtering, consumer protection, individual privacy, and digital copyright.[71] In 2018, the EU enforced the General Data Protection Regulation (GDPR), extending digital privacy to all of its citizens, limiting the export of personal data outside the EU, and unifying national regulations within the EU.[72] Since 2009, the Lisbon Treaty has strengthened the EU's security credentials by increasing the Council's authority to define a common approach to foreign threats, and, under a mutual defense clause, oblige all member states to provide help to any other member under attack.[73] Cybersecurity is currently a hot topic, with smaller countries often leading the way: For example, Lithuania is in charge of the new EU project called Cyber Rapid Response

69 This is a personal observation, having attended international cyber-norms conferences both at Moscow State University and at MIT for over ten years. For more background, see: Franz-Stefan Gady and Greg Austin, *Russia, the United States, and Cyber Diplomacy: Opening the Doors*, EastWest Institute, 2010, https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf.

70 The EU has a gross domestic product (GDP) larger than China and second only to the United States. "GDP (current US$)," World Bank national accounts data and Organisation for Economic Co-operation and Development National Accounts data files, World Bank website, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-US-CN.

71 The Budapest Convention is supplemented by the Protocol on Xenophobia and Racism committed through computer systems. "Budapest Convention and Related Standards," Council of Europe website, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

72 "The EU General Data Protection Regulation (GDPR)," https://eugdpr.org/.

73 "The Treaty of Lisbon," Fact Sheets on the European Union, European Parliament website, http://www.europarl.europa.eu/factsheets/en/sheet/5/the-treaty-of-lisbon.

Teams and Mutual Assistance in Cyber Security. Part of Permanent Structured Cooperation (PESCO), the Teams focus on the technically (and politically) challenging discipline of incident response during a crisis.[74]

In terms of a credible military alliance, there is only one: NATO, whose purpose since 1949 has been the collective defense of all its member countries. NATO not only encompasses Europe and North America, but also comprises dozens of other nations across the globe through the Euro-Atlantic Partnership Council, Mediterranean Dialogue, Istanbul Cooperation Initiative, and Contact Countries.[75] On cybersecurity, NATO has been in high gear since the attack on Estonia in 2007. The 2010 NATO Strategic Concept described cyberattacks as threatening "Euro-Atlantic prosperity, security and stability."[76] In 2014, the allies declared that cyber defense is now a core part of collective defense, and that a cyberattack could lead to the invocation of Article Five,[77] which is NATO's core organizing principle of collective defense and states that an attack against one ally is an attack against all allies.[78] In 2016, NATO recognized cyberspace as a domain of operations in which the Alliance will "defend itself as effectively as it does in the air, on land, and at sea." In 2018, the allies agreed to establish a Cyberspace Operations Centre from which NATO can leverage its members' national cyber capabilities for allied missions and operations.[79]

Finally, we must remember that cybersecurity is a strategic, multifaceted challenge, which neither a political agreement nor a military alliance can fully address alone. Fortunately, the EU and NATO have long recognized that they must collaborate if they are to overcome national security challenges to their common geography, commitment to democracy, and respect for the rule of law. Twenty-two countries are members of both organizations (a majority in both). In 2002, the EU and NATO signed the European Security and Defence Policy (ESDP), specifying "shared values," "indivisible" security, and a determination to tackle "new century" challenges together.[80] In 2010, they determined to improve their strategic partnership;[81] in 2016, they issued a joint declaration covering cybersecurity, hybrid threats, and capacity-building efforts,[82] and expanded this agreement in 2018.[83] In 2017, the EU and NATO opened the European Centre of Excellence for Countering Hybrid Threats in Helsinki, Finland[84]—a critical step in recognizing the growing complexity of cybersecurity as a national security issue.[85]

---

74 "PESCO Projects: Cyber Rapid Response Teams and Mutual Assistance in Cyber Security," referring to the EU's permanent structured cooperation projects, https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.

75 Geers, "Kosovo, Cyber Security, and Conflict Resolution."

76 "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon," NATO, November 19, 2010, and last updated May 23, 2012, https://www.nato.int/cps/en/natohq/official_texts_68580.htm.

77 "NATO's Role in Cyberspace," NATO, February 12, 2019, https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm.

78 "Collective Defence—Article 5," NATO, June 12, 2018, https://www.nato.int/cps/en/natohq/topics_110496.htm.

79 "Cyber Defence," NATO, September 6, 2019, https://www.nato.int/cps/en/natohq/topics_78170.htm.

80 "EU-NATO Declaration on ESDP," December 16, 2002, https://www.nato.int/cps/en/natolive/official_texts_19544.htm.

81 "Relations with the European Union," NATO, August 12, 2019, https://www.nato.int/cps/en/natohq/topics_49217.htm.

82 "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf. See also: "EU-NATO Cooperation—Factsheets," European Union, June 11, 2019, https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en.

83 "Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf.

84 The European Centre of Excellence for Countering Hybrid Threats, Helsinki, Finland, https://www.hybridcoe.fi/.

85 Again, cyberattacks have been used to facilitate hostile action against targets as diverse as electricity grids and elections.

4. CASE STUDY
DEFENDING DEMOCRACY IN UKRAINE[85]

An Allied approach to cybersecurity sounds good in theory, but proof can only be found in real-world practice. Above, we saw that many of the most famous cyberattacks in history have occurred within the former Soviet Union and Warsaw Pact countries. In 2020, this is still true, as the current ground zero for geopolitical cyberattacks is Ukraine, which Russia invaded following the Euromaidan Revolution in 2014. The most recent Ukrainian presidential election, which took place in 2019, offers a powerful argument for international collaboration on cybersecurity.

As the Euromaidan movement began, cyberattacks rose in parallel with political tension. In 2012, hackers "defaced" Ukrainian government websites with "digital graffiti."[87] In 2013, they deployed highly aggressive malware like RedOctober, MiniDuke, and NetTraveler. In 2014, hacktivists leaked stolen Ukrainian government documents.[88] When Ukrainian protesters took to the streets to rail against then-President Viktor Yanukovych's scrapping of an EU treaty, there were cyber and physical attacks "against opposition servers, smartphones, websites, and Internet accounts."[89] During the invasion of Crimea, Russian special operations forces severed network cables, commandeered satellites, and made wholesale changes to conflict-related pages on Wikipedia.[90] In Donbass, cyber espionage has targeted Ukrainian army units (e.g., location data from mobile phones and Wi-Fi networks), and Ukrainian citizens living there have been isolated from Kyiv via Internet censorship and routine forensics checks on computers and mobile devices.[91]

In May 2014, Ukraine's Computer Emergency Response Team (CERT-UA) reported on the "most technically advanced attack" it had ever investigated: the compromise of Ukraine's Central Election Commission (CEC), which is believed to have been part of a coordinated Russian effort to discredit Ukrainian democracy.[92] In hindsight, this attack should have been a warning to Washington, which suffered its own coordinated Russian cyberattack against the 2016 US presidential election.[93]

Since 2014, as its conflict with Russia has continued, cyberattacks against Ukraine have only increased in severity. In 2015, hackers manipulated Ukraine's power grid, leaving over 300,000 people in the dark during the Christmas holiday.[94] In 2016, almost exactly one year later, the same hackers returned, with a power supply cut that appeared to taunt Ukrainian cyber defense and national security staff.[95] In 2017, Ukraine was hit by the costliest cyberattack in world history, "Not-Petya," in which the Ukrainian government, banks, newspapers, and electricity firms (as well as foreign firms doing business in Ukraine) were struck by malicious code that was intended to cause maximum damage to

86 Many thanks to Igor Pigariev and Laura Galante, who co-authored parts of this section in support of the Atlantic Council's Ukraine Election Task Force (https://ukraineelects.org/). I also presented our case study findings in a white paper titled "Ukraine 2019: Kudos to Cyber Defense or Lucky Strike?," at the "Cyber Norms 7.0" conference, MIT, April 2019.

87 Kenneth Geers, "Cyber War in Perspective," introduction to *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Geers, NATO CCDCOE Publications, (December 2015), https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf.

88 Nikolay Koval, "Revolution Hacking," in *Cyber War in Perspective*, ed. Geers.

89 Geers, "Cyber War in Perspective," introduction to *Cyber War in Perspective*.

90 The most serious cyber incidents coincided with the lethal shooting of activists.

91 Glib Pakharenko, "Cyber Operations at Maidan: A First-Hand Account," in *Cyber War in Perspective*, ed. Geers.

92 Koval, "Revolution Hacking."

93 United States v. Netyksho, Antonov, Badin, Yermakov, Lukashev, Morgachev, Kozachek, Yershov, Malyshev, Osadchuk, Potemkin, and Kovalev.

94 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

95 Andy Greenberg, " 'Crash Override': The Malware That Took Down a Power Grid," *Wired*, June 12, 2017, https://www.wired.com/story/crash-override-malware/.

enterprises.[96] In 2020, Not-Petya has businesses and insurance firms around the world fighting over billions of dollars.[97] Given that the US government has blamed the attack on the Russian military,[98] this incident may be seen as an act of war. In 2018, the Netherlands expelled four Russian cyber spies who tried to hack information related to the downing of Malaysia Airlines Flight 17 (MH-17), which took off from Amsterdam and was shot down over Ukraine by suspected Russia-backed military forces.[99]

In the face of so many destructive cyberattacks, the Ukrainian government spared no effort to defend the integrity of its 2019 presidential election. For Kyiv, the credibility of democracy was at stake. Prior to the vote, national security leadership issued a series of warnings: Yehor Bozhok, the head of Ukraine's Foreign Intelligence Service, said that Russia had allocated US$350 million to destabilize Ukraine and meddle in its election;[100] Serhiy Demedyuk, chief of Ukraine's cyber police, warned that well-known Russian hacker groups such as Fancy Bear and the Shadow Brokers were active in Ukraine and scaling up their operations;[101] and finally, Oleksandr Klymchuk, cybersecurity chief at the Security Service of Ukraine (SBU), opined that Russia may choose to disrupt national critical infrastructures like transport, communications, finance, or energy, in an effort to disrupt the poll.[102]

To bolster national cyber defenses, all government agencies took part. The "Concept of Preparation for Repelling Military Aggression in Cyberspace" was published to help counter hybrid war, support defense sector reform, and achieve interoperability with NATO.[103] The Verkhovna Rada, Ukraine's legislature, allocated higher funding for the Central Election Commission (CEC)[104] and created a twenty-four-hour working group devoted to securing CEC information resources.[105] Ukraine began to share its cyber threat intelligence with the world via the Malware Information Sharing Platform-Ukraine (MISP-UA).[106] SBU chief Vasyl Hrytsak announced that law enforcement would do everything in its power to ensure election security.[107] The National Center for Cyber Security was established to coordinate all of these activities.[108] In the end, CEC Chair Tetiana Slipachuk announced that Ukraine was ready on a "moral and technical level to respond to the challenges."[109]

In sum, these Ukrainian efforts were truly impressive. But the fact remains that no nation today can successfully address the cybersecurity challenge alone. With this in mind, the EU and NATO provided substantial support to Kyiv throughout its 2019 election. The European Police Office (Europol) announced that the damage wrought by NotPetya (believed to be

96 Greenberg, "The Untold Story."

97 "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong," *New York Times*, April 15, 2019, https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.

98 Ellen Nakashima, "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, January 13, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

99 "How the Dutch Foiled Russian 'Cyber-attack' on OPCW," BBC News, October 4, 2018, https://www.bbc.com/news/world-europe-45747472.

100 "Ukraine's Foreign Intel Service: Russia to Spend US$350 Million for Meddling in Ukraine Elections," UNIAN, January 25, 2019, https://www.unian.info/politics/10421127-ukraine-s-foreign-intel-service-russia-to-spend-us-350-mln-for-meddling-in-ukraine-elections.html.

101 "Russian Hackers Scaled Up Activity in Ukraine Cyber Space Ahead of Election," Institute Mass Information, March 18, 2019, https://imi.org.ua/en/news/russian-hackers-scaled-up-activity-in-ukraine-cyber-space-ahead-of-election/.

102 "Ukraine's SBU to Block Websites Threatening National Security," UNIAN, February 12, 2019, https://www.unian.info/politics/10443432-ukraine-s-sbu-to-block-websites-threatening-national-security.html.

103 "Oleksandr Turchynov: Russia Is Going to Use the Entire Arsenal, Including Cybernetic Means, to Influence the Democratic Will of the Ukrainian People," National Security and Defense Council of Ukraine, February 19, 2019, http://www.rnbo.gov.ua/en/news/3213.html.

104 "Oleksandr Turchynov: Russia is Going to Use the Entire Arsenal."

105 "VR Approves Bill on Strengthening Cybersecurity of Central Election Commission," UKRINFORM, November 22, 2018, https://www.ukrinform.net/rubric-polytics/2585074-vr-approves-bill-on-strengthening-cybersecurity-of-central-election-commission.html.

106 "СБУ запустила платформу по противодействию кибератакам на выборах 2019 года," РБК-Украина, November 14, 2018, https://www.rbc.ua/rus/news/sbu-zapustila-platformu-protivodeystviyu-1542195394.html.

107 "SBU Head Hrytsak Accuses Russia of Playing 'Religious Card' in Ukraine for Interference in Electoral Process," Interfax-Ukraine, February 18, 2019, https://en.interfax.com.ua/news/general/566923.html.

108 "Ukraine Creates National Center for Cyber Security," UNIAN, June 8, 2016, https://www.unian.info/society/1369157-ukraine-creates-national-center-for-cyber-security.html.

109 "Central Election Commission Ready to Respond to Russia's Meddling in Elections," UKRINFORM, March 31, 2019, https://www.ukrinform.net/rubric-elections/2670946-central-election-commission-ready-to-respond-to-russias-meddling-in-elections.html.

of Russian origin) and WannaCry (likely from North Korea) proved that existing cyber defenses are insufficient, and that more must be done to protect Europe.[110] In March, close to one hundred Western experts took part in cybersecurity exercises with the SBU and Ukraine's State Special Communication Service (SSCS). The CEC received new training, hardware, and software. Professional red teams[111] from abroad launched simulated cyberattacks against Ukraine, and local experts sought to neutralize them.[112] With EU parliamentary elections scheduled just weeks after the Ukrainian poll,[113] Europe was keen not only to help Kyiv but also to learn the latest attack tools and techniques. Then-UK Defence Secretary Gavin Williamson explained that Russia was trying to bring former Soviet states "back into its orbit," fighting in a "gray zone" short of war in which cyberattacks were a primary weapon. He further warned that the cost of failing to address Russian aggression was "unacceptably high."[114]

Support from Washington came in multiple forms. In 2018, the US State Department pledged US$10 million in cybersecurity aid to Ukraine.[115] In February 2019, then-President of Ukraine Petro Poroshenko announced that the United States had helped Ukraine to stop a Russian DDoS against the CEC.[116] In a speech, former US Director of National Intelligence James Clapper said Moscow had not only meddled in Ukraine's democracy in 2014 and in the US 2016 elections, but had tested a broad range of attacks against Ukraine, from social media manipulation to power grid compromise.[117] On the day of the 2018 US midterm election, in an event that could easily have had ramifications in Ukraine, the US Cyber Command conducted a DoS cyberattack against the Russian Internet Research Agency, partly in retaliation for its interference in the 2016 US presidential election, and partly to warn that similar operations would not be tolerated in the future.[118]

Today, even the private sector is engaged in international cybersecurity efforts.[119] In January 2019, Facebook announced a new initiative to promote transparency in political advertising, including the indexing of its ads in a searchable online library. Its primary goal was to make it difficult for foreign intelligence services to run political ads in other countries.[120] In March, Facebook announced an outright ban on foreign political advertising in Ukraine's electoral campaign, in order to minimize the illicit promotion of politicians, parties, slogans, and symbols, and the company said that it would henceforth employ both automated and human analysis to safeguard election integrity around the world.[121]

---

110 "Law Enforcement Agencies across the EU Prepare for Major Cross-border Cyber-attacks," European Union Agency for Law Enforcement Cooperation, March 18, 2019, https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks.

111 Red teams consist of security personnel who are hired to test how well an organization might fare in the face of a real attack.

112 "Ukraine Ready to Take on Russian Election Hackers," *Security Week*, March 18, 2019, https://www.securityweek.com/ukraine-ready-take-russian-election-hackers.

113 European Parliament elections took place on May 23–26, 2019.

114 "Resurgent Russia Aims to Bring Ukraine Back Into Its Orbit–UK Defense Secretary," UNIAN, February 11, 2019, https://www.unian.info/world/10442427-resurgent-russia-aims-to-bring-ukraine-back-into-its-orbit-uk-defense-secretary.html.

115 "Second US-Ukraine Cybersecurity Dialogue," US Department of State, Office of the Spokesperson, November 5, 2018, https://ua.usembassy.gov/second-u-s-ukraine-cybersecurity-dialogue/.

116 Sean Lyngaas, "Ukraine's President Accuses Russia of Launching Cyberattack against Election Commission," *Cyberscoop*, February 26, 2019, https://www.cyberscoop.com/ukraines-president-accuses-russia-launching-cyberattack-election-commission/.

117 "General James Clapper: Russia Uses Techniques Tested in Ukraine to Meddle in US Elections," UKRINFORM, February 22, 2019, https://www.ukrinform.net/rubric-polytics/2645968-general-james-clapper-russia-uses-techniques-tested-in-ukraine-to-meddle-in-us-elections.html.

118 Andy Greenberg, "US Hackers' Strike on the Russian Trolls Sends a Message—But What Kind?," *Wired*, Feb 27, 2019, https://www.wired.com/story/cyber-command-ira-strike-sends-signal/.

119 One prominent example is Microsoft's "Digital Geneva Convention." See: "A Digital Geneva Convention to Protect Cyberspace," Microsoft Policy Papers, Microsoft website, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.

120 Dave Paresh, "Exclusive–Facebook Brings Stricter Ads Rules to Countries with Big 2019 Votes," Reuters, January 16, 2019, https://uk.reuters.com/article/uk-facebook-elections-exclusive/exclusive-facebook-brings-stricter-ads-rules-to-countries-with-big-2019-votes-idUKKCN1PA0C6.

121 "Facebook Prohibits Foreign-funded Ads for Ukraine Election–Media," UNIAN, March 5, 2019, https://www.unian.info/politics/10468851-facebook-prohibits-foreign-funded-ads-for-ukraine-election-media.html.

Euromaidan in Kyiv, 2014. *Photo credit*: Ввласенко/Wikimedia Commons.

Despite all of these efforts, there were still many publicly known cybersecurity incidents during Ukraine's 2019 presidential election. Here is a high-level summary:

JANUARY

- Hacktivists leak thousands of alleged Russian government files revealing possible Russian covert activities in Ukraine.[122]
- Hackers conduct a phishing campaign against CEC employees, sending greeting cards, shopping invitations, and software update notices laced with malware.[123]
- Ukraine's Cyber Police discover the purchase, on the darknet with cryptocurrency, of stolen personal data belonging to CEC employees, allegedly with money provided by Russian special services.[124]

FEBRUARY

- Ukraine's National Security and Defense Council blocks two thousand suspicious accounts and two hundred websites promoting Russian ideology.[125]
- An http "flood" DoS attack (exploiting an outdated version of WordPress) targets the CEC and blocks access to its employees.[126]

MARCH

- The SBU arrests four Ukrainians for spreading negative information about the election in social media, receiving payment via banned online

122 Stefan Jajecznyk, "The Dark Side of the Kremlin: Hacked Russian Documents Explained," Al Jazeera, February 26, 2019, https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html.

123 Pavel Polityuk, "Exclusive: Ukraine Says It Sees Surge in Cyber Attacks Targeting Election," Reuters, January 25, 2019, https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-it-sees-surge-in-cyber-attacks-targeting-election-idUSKCN1PJ1KX.

124 Polityuk, "Exclusive: Ukraine."

125 "Ukraine's SBU to Block Websites Threatening National Security," UNIAN, February 12, 2019, https://www.unian.info/politics/10443432-ukraine-s-sbu-to-block-websites-threatening-national-security.html.

126 "SBU Blocks Large-scale Cyberattack on CEC Website," UKRINFORM, February 27, 2019, https://www.ukrinform.net/rubric-society/2649609-sbu-blocks-largescale-cyberattack-on-cec-website.html.

money transfer services, and taking "orders" from Russia.[127]

- Ukrainian Cyber Police announce hackers based in Russia had disseminated fraudulent "official" emails favoring one Ukrainian presidential candidate and falsely claiming CEC legal violations.[128]
- On Russian television, a former Ukrainian intelligence officer claims that Kyiv can control its electronic voting system and would manipulate election results to favor the incumbent.[129]
- Facebook removes 1,907 pages, groups, and accounts, linked to Russia, for engaging in spam and coordinated "inauthentic" behavior.[130]
- A massive distributed DDoS attack knocks election front-runner Volodymyr Zelenskiy's website off-line.[131]
- Ukraine's Cyber Protection Centre announces that hackers tried to penetrate national critical infrastructures and suggests that in some cases they did gain access.[132]
- Russian agents allegedly attempt to pay Ukrainians for access to their social media accounts, in order to more easily spread disinformation and promote false narratives within Ukraine.[133]
- A senior Russian official states that Moscow was concerned about the potential falsification or misuse of Ukrainian citizens' personal data.[134]
- Ukraine's Cyber Police describe attempts to discover vulnerabilities on a CEC web server via compromised routers in Ukraine that Kyiv says were hacked from Russia.[135]

APRIL

- The CEC publishes first round results, stating that cyberattacks were conducted on CEC systems, but that they did not affect the process of determining the first round winner.[136]
- Ukraine's security services investigate whether Zelenskiy's campaign received financing from Russia, as suggested by a tranche of hacked emails.[137]
- Facebook official David Agranovich says Russia tested election interference methods in Ukraine

127 "Security Service Exposes Anti-Ukrainian Agitators from Mykolaiv, Odesa," 112.International news platform (part of 112.UA), March 21, 2019, https://112.international/politics/security-service-exposes-anti-ukrainian-agitators-from-mykolaiv-odesa-38028.html.

128 "Russian Hackers Send Emails on Behalf of Ukrainian Interior Minister," 112.UA news agency, March 22, 2019, https://112.international/politics/russian-hackers-send-emails-on-avakovs-behalf-with-fake-rules-during-elections-38081.html.

129 "Russian TV Brandishes 'SBU defector'," LB.UA, March 25, 2019, https://en.lb.ua/news/2019/03/25/7164_russian_tv_brandishes_sbu_defector.html.

130 Ron Synovitz, "Facebook Removes Hundreds of Accounts from Russia, Iran, North Macedonia, Kosovo," Radio Free Europe/Radio Liberty, March 26, 2019, https://www.rferl.org/a/facebook-removes-hundreds-of-accounts-from-russia-iran-macedonia-kosovo/29843067.html.

131 David Gilbert, "Inside the Massive Cyber War between Russia and Ukraine," *Vice News*, March 29, 2019, https://news.vice.com/en_us/article/bjqe8m/inside-the-massive-cyber-war-between-russia-and-ukraine.

132 Gilbert, "Inside the Massive Cyber War."

133 Michael Schwirtz and Sheera Frenkel, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering," *New York Times*, March 29, 2019, https://www.nytimes.com/2019/03/29/world/europe/ukraine-russia-election-tampering-propaganda.html.

134 "Russian MP Concerned over Reports of Possible Falsifications during Ukrainian Election," TASS Russian News Agency, March 31, 2019, http://tass.com/politics/1051333.

135 Jack Laurenson, "Disrupt and Discredit: Russia Still Has Ukrainian Elections in Sights," *Kyiv Post*, April 1, 2019, https://www.kyivpost.com/ukraine-politics/disrupt-and-discredit-russia-still-has-ukrainian-elections-in-sights.html; "Аваков розповів про кібератаки на сервера ЦВК у день виборів," РБК-Україна, April 2, 2019, https://www.rbc.ua/ukr/news/avakov-rasskazal-kiberatakah-servera-tsik-1554164761.html.

136 "Вибори президента України-2019: офіційні результати," 24 Канал, April 23, 2019, https://24tv.ua/vibori_2019_ukrayina_rezultati_golosuvannya_na_viborah_prezidenta_ofitsiyni_n1132956; "Аваков розповів про кібератаки на сервера ЦВК у день виборів," РБК-Україна, April 2, 2019.

137 Cristina Maza, "Hacked Emails Appear to Reveal Russia Is Backing Comedian Likely to Be Ukraine's Next President," *Newsweek*, April 17, 2019, https://www.newsweek.com/ukraine-russia-president-election-volodymyr-zelenskiy-1399563.

for use against democracies worldwide, in order to undermine "public trust."[138]

- Ukraine's National Police announce that "unlawful interference in the electronic systems of the Central Election Commission has not been recorded" during the second round.[139]

Even in retrospect, it is hard to write a definitive account of the state of cybersecurity in Ukraine during its 2019 presidential election. First, although there was no major cyberattack, the numerous incidents described above could easily have been more impactful in a closer election. As it happened, Zelenskiy won the race by a wide margin. Second, there were no serious pro-Moscow candidates in this race, so the best that the Kremlin could hope for was to damage the integrity of democracy itself (as in 2014). That said, it is nonetheless important to credit all of the domestic and international initiatives undertaken to secure Ukraine's critical infrastructure and information space as a crucial step in promoting and securing democracy worldwide. Hackers will doubtless try to sway countless future elections, but cyber defenders can look back on Ukraine's 2019 election for insight and inspiration.

---

138 Стас Юрасов, Евгений Шишацкий, "Экс-директор разведки СНБ США: ольгинские тролли атакуют Украину," Лига.tech, April 19, 2019, https://tech.liga.net/technology/interview/eks-direktor-razvedki-snb-ssha-olginskie-trolli-atakuyut-ukrainu.

139 "National Police: No Cyberattacks on CEC Systems Recorded During Second Round of Elections," UKRINFORM, April 25, 2019, https://www.ukrinform.net/rubric-elections/2688206-national-police-no-cyberattacks-on-cec-systems-recorded-during-second-round-of-elections.html.

5. CONCLUSION

In 1948, Hans Morgenthau wrote that a nation's security depends on the integrity of its borders and institutions.[140] But every day, the global nature of the Internet challenges borders and institutions in new and surprising ways. Today, there is a clear relationship between network security and national security. And as IT is launched into space,[141] and in miniature invades the human body,[142] our cybersecurity challenges will only grow more profound over time.[143]

Nations now face a paradox: They cannot disconnect from the Internet for fear of losing its benefits; yet the nature of cyberspace allows adversaries to commit crime,[144] espionage, terrorism, and war, on their sovereign territory. Every conflict now has a digital dimension, whose size and impact are hard to predict, while law enforcement jurisdiction ends every time a network cable crosses a national border. Governments are so limited in what they can achieve, in fact, that cybersecurity (like global warming or a pandemic) is fundamentally an international problem that requires an international solution.

The moral of this story is clear: In the Internet era, allies have never been more important. The power of IT will hopefully lead to a more peaceful world. However, the intractability of traditional geopolitics, and the specter of increasingly powerful cyberattacks, suggest that all nations are likely to invest significant sums in cyberattack as a military weapon, both for proactive deterrence and potential retaliation. Given the limitations of any single nation-state in the digital domain, we are therefore likely to see tangible cybersecurity progress (at least in the near term) only within political and military alliances. **Indeed, the only credible cyber superpower is a robust alliance.**

Russia and China offer a model that is attractive to authoritarian regimes. The aggressive behavior of Moscow and Beijing in cyberspace—both domestically and in other countries—will likely repel more nations than it will attract. Many of the cyberattacks described in this paper were sponsored by the Kremlin, but as China invests heavily in digital infrastructure worldwide, Beijing may ultimately be a greater cyber threat to the West.

The EU and NATO already have numerous strategic cybersecurity accomplishments to their credit, and it is within these political and military alliances that we are most likely to see future progress. Any nation truly wanting to improve its cybersecurity—and economy, democracy, rule of law, and human rights—should collaborate with the EU and NATO, which benefit not only from size and wealth but also diversity. In fact, many of their newest, smallest member states have borne the brunt of Russia's cyberattacks. They are therefore ideally positioned to shine a light on the latest cybersecurity threats, which are often seen there first, before appearing in other parts of the world.

---

140 H. J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace* (New York: Alfred A. Knopf, 1948), 440.

141 Malcolm Davis, "The Cyber Threat to Satellites," Australian Strategic Policy Institute, September 9, 2019, https://www.aspistrategist.org.au/the-cyber-threat-to-satellites/.

142 Sigal Samuel, "How Biohackers Are Trying to Upgrade Their Brains, Their Bodies—and Human Nature," *Vox*, June 25, 2019, https://www.vox.com/future-perfect/2019/6/25/18682583/biohacking-transhumanism-human-augmentation-genetic-engineering-crispr.

143 Military cyber commands are already compromising targets that are neither connected to the Internet nor accessible through traditional, IP-based hacking operations. See: Mark Pomerleau, "The New Electronic Warfare Tool Cyber Units Will Need," *Fifth Domain*, April 27, 2019, https://www.fifthdomain.com/dod/2019/04/26/the-new-electronic-warfare-tool-cyber-units-will-need/.

144 Examples include Internet fraud, credit-card fraud, bank-card skimming, the dissemination of child pornography, etc. One spectacular example is North Korea's bank robberies via the Internet. See: Patrick Winn, "How North Korean Hackers Became the World's Greatest Bank Robbers," GlobalPost Investigations, Public Radio International, May 16, 2018, https://gpinvestigations.pri.org/how-north-korean-hackers-became-the-worlds-greatest-bank-robbers-492a323732a6.

6. RECOMMENDATIONS

IT is now a rapidly evolving and often unpredictable discipline. Nation-state computer network operations are closer to special forces or "black ops" than they are to traditional military operations, and are often hidden behind layers of classification. Nonetheless, within the context of a democratic alliance, we have no choice but to collaborate: The race is on to secure international norms for cyberspace, and the EU and NATO have no time to lose. We must work with old, new, and future member states to create a common cyber defense framework for the world.

Here are four recommendations to promote trust and collaboration among EU and NATO member states and partners:

INTELLIGENCE SHARING AND TRANSPARENCY

Cyber intelligence is notoriously technical and time sensitive. However, it also can be highly actionable. Even sharing a single, well-chosen indicator of compromise[145] can shed valuable light on a cyber incident, campaign, or the actor behind them. Attacker infrastructure, personnel, and operations are finite; proactively sharing adversary tactics, techniques, and procedures (TTP) throughout an alliance offers strategic force multiplication that can preempt many future cyberattacks. In fact, the US Cyber Command has been publicly releasing an increasing amount of intelligence related to hostile nation-state operations.[146] The United States is not alone in recognizing that transparency and publicity of cyber threats is key to a broader public understanding of the challenge. The Lithuanian Ministry of National Defense releases an annual National Cyber Security Status Report detailing the actions it has taken to increase cybersecurity as well as statistics on the types of cyber challenges faced by Lithuania. The goal of this report, and others like it, is to "inspire…at least one person to take care of cyber security in her or his own immediate environment…" and thereby increase the overall cybersecurity of the country.[147] Similar efforts by other allies to raise public awareness around cybersecurity issues could create a more resilient alliance when facing cyber threats.

JOINT INVESTIGATIONS

Even a first-tier intelligence service is surprisingly limited in its funding, personnel, resources, and time—not to mention that cybersecurity talent get paid far better in the private sector. However, in the context of a robust alliance, it is possible for literally dozens of national-level network security, law enforcement, and intelligence agencies to sing from the same sheet of music.[148] Because the digital domain is so democratic, even small alliance members—from Luxembourg to Lithuania—regularly make major contributions, in both investigation and response.[149] One key will be to develop clear, common standards for what constitutes a digital crime, as well as sufficient evidence to prove it.

JOINT ATTRIBUTION

The unique nature of many cyberattacks, as well as the fact that few of them rise to the level of a true national security threat,[150] complicates cyber

145 Common technical indicators include an IP address, domain name, or malware hash used by an attacker.

146 Shannon Vavra, "Cyber Command's Biggest VirusTotal Upload Looks to Expose North Korean-linked Malware," *Cyberscoop*, September 8, 2019, https://www.cyberscoop.com/cyber-command-virus-total-north-korean-malware/; Joseph Cox, "Internal Docs Show Why the U.S. Military Publishes North Korean and Russian Malware," February 25, 2020, Motherboard, a Vice online magazine and video channel, https://www.vice.com/en_us/article/5dmwyx/documents-how-cybercom-publishes-russian-north-korean-malware-virustotal.

147 National Cyber Security Centre, *National Cyber Security Status Report 2019*, Ministry of National Defense of Lithuania, 2019, https://www.nksc.lt/doc/en/NKSC_2019_EN.pdf.

148 In my twenty years working for the US Department of Defense, including time at the National Security Agency, NCIS, and NATO, I can tell you that little gets done in the real world without international partners.

149 Cybersecurity Competence Center (C3), Luxembourg, https://www.c-3.lu/. For example, Lithuania's National Cyber Security Centre, under its Ministry of National Defence, now publishes a stellar annual National Cyber Security Status Report (https://www.nksc.lt/doc/en/NKSC_2018_EN.pdf). It would be ideal to link, if not combine, the independent threat assessments from all EU and NATO member states and their international partners.

150 For a variety of reasons, including the difficulty of damage assessment, the uncertainty of attribution, and a generally bloodless character, an awareness of the vast majority of cyberattacks will never reach the highest levels of government.

defense in numerous ways, such as knowing how to respond with discretion and proportionality.[151] Often, however, the biggest stumbling block is credible attribution. Many times, the best response (beyond mitigating technical vulnerabilities) has simply been to name and shame the attacker. The United States has done this against four nations: Russia,[152] China,[153] Iran,[154] and North Korea.[155] But attribution coming from one nation (even a great power) pales in comparison to attribution from an alliance, comprising dozens of nations, many more data points as evidence, and a greater potential for concrete response.

LIMITATION ON CYBER ESPIONAGE WITHIN EU/NATO

There is a fine line between cyber espionage (e.g., reading hacked emails) and cyberattack (e.g., deleting or changing the content of those emails). Not only is it difficult to tell these two activities apart, but the former can quickly morph into the latter. On cyber defense, therefore, we often have to assume the worst, which makes cyber espionage an unhealthy dynamic within the context of an alliance. By limiting cyber espionage among EU and NATO allies, like-minded democracies can kill two birds with one stone: 1) build trust, and 2) isolate real adversaries. This recommendation may be the most difficult to follow in the short term,[156] but may ultimately be the most rewarding.

---

151 "What Are the Rules of War and Why Do They Matter?" The International Committee of the Red Cross, October 19, 2016, https://www.icrc.org/en/document/what-are-rules-of-war-Geneva-Conventions.

152 "Russian Interference in 2016 US Elections," Federal Bureau of Investigation, https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections.

153 "Chinese Hackers Indicted," Federal Bureau of Investigation, December 20, 2018, https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018.

154 "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," US Department of Justice, March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

155 "North Korean Regime-backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," US Department of Justice, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

156 Espionage is always a tricky business, even among allies. See: Julia Edwards, "Obama Acknowledges Damage from NSA Eavesdropping on Merkel," Reuters, February 9, 2015, https://www.reuters.com/article/us-usa-spying-obama/obama-acknowledges-damage-from-nsa-eavesdropping-on-merkel-idUSKBN0LD28N20150209; and Greg Miller, "The Intelligence Coup of the Century," *Washington Post*, February 11, 2020, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

5. ABOUT THE AUTHOR

Dr. Kenneth Geers works at Very Good Security. He is an Atlantic Council Cyber Statecraft Initiative Senior Fellow within the Scowcroft Center for Strategy and Security, a NATO Cooperative Cyber Defence Centre of Excellence Ambassador, and a Digital Society Institute-Berlin Affiliate. Kenneth served for twenty years in the US Government: in the Army, National Security Agency (NSA), Naval Criminal Investigative Service (NCIS), and NATO. He is the author of *Strategic Cyber Security*, editor of *Cyber War in Perspective* and *The Virtual Battlefield*, and technical expert to the *Tallinn Manual*.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org