Colin

The cyber sphere presents new challenges that the EU and NATO must address.

European Union and NATO Global Cybersecurity Challenges

A Way Forward

BY LUUKAS K. ILVES, TIMOTHY J. EVANS, FRANK J. CILLUFFO, AND ALEC A. NADEAU

Over the past two decades, European countries have had to meet the same cybersecurity challenges that the United States has faced. However, while the U.S. has benefitted from its sovereign authority (a single foreign policy, a centralized military, and the legal and budgetary power of the federal government), European governments have had to take steps to develop cybersecurity policies at the national level while simultaneously pooling their sovereignty through the North Atlantic Treaty Organization (NATO) and the European Union (EU) to bolster their defenses.

This article describes the approaches that NATO and the EU currently use to defend their members' interests against such threats. In the last decade, both organizations have recognized that cybersecurity is a key challenge to their core objectives, and they have adopted increasingly ambitious strategies, established new organizations, and (in the EU's case) promulgated legislation to address these threats. Specifically, NATO and the EU have begun to come to terms with the fact that all major security conflicts going forward will have both a cyber and a kinetic component. Cybersecurity failures will increasingly be equivalent to or indicative of broader national security failures. These failures will also lead to the degradation of economic and privacy interests within the member states of NATO and the EU. This reality is forcing all international diplomatic and security-focused organizations, alliances, and associations to retool existing structures or to create new ones through which they can achieve cyber defense and cybersecurity goals.

Luukas Ilves is Counselor for Digital Affairs at the Permanent Representation of Estonia to the EU. Timothy Evans is Senior Advisor, Cyber Strategy and Policy, at Johns Hopkins University Applied Physics Laboratory in Arlington, Virginia. Frank Cilluffo is the Director of the George Washington University's Center for Cyber and Homeland Security. Alec Nadeau is a Presidential Administrative Fellow at the George Washington University's Center for Cyber and Homeland Security. ***The authors would like to thank Liina Areng and Liga Rozentale for their contributions to this article.***

Three of the most prominent examples of cyber aggression between nation-states are those on Estonia (2007), Georgia (2008), and Ukraine (2014, 2015) by Russia and its proxies. In 2007, Russian nationals launched sustained Distributed Denial of Service (DDoS) attacks against Estonia that disrupted the Web services of the Estonian government and private sector for weeks.[1] The following year, three weeks prior to kinetic hostilities, Russia's conflict with Georgia over South Ossetia began in cyberspace with DDoS attacks and Website defacements that later blended into Russia's overall warfighting strategy.[2] Finally, in 2014 Russia and Ukraine were engaged in cyber attacks, integrated alongside physical conflict that targeted government and media infrastructure, contributing to the fog of war surrounding Russia's annexation of Crimea.[3] Russia squared off against its neighbor again in December 2015 when it attacked Ukraine's electric grid and subsequently launched DDoS attacks, which left 230,000 residents without power for up to 6 hours.[4] These examples demonstrate not only a growing threat to European security from an increasingly aggressive Russia, but also the trend toward a single concept of conflict that makes cyber and kinetic aggression inseparable. It is important to note that China, Iran, and North Korea, to varying extents, also have the capability and intent to threaten the security of NATO and EU member states through cyber means.[5]

Developments in the cybersecurity operations of both NATO and the EU have paralleled the growth of cybersecurity as a major policy concern to the United States and other national governments. The digital revolution has also changed the basic environment in which governments operate, necessitating increasing levels of cross-border interdependence and connectivity. European countries have responded to the need to increase coordination and cooperation through new initiatives at the national level and under the auspices of NATO and the EU. Nevertheless, the relationship between national capabilities and sovereignty, and the authority of these two international organizations, remains unsettled. The efforts of NATO and the EU to mainstream cybersecurity into existing activities have thus far proven insufficient to fully address the growing cyber threat landscape.

NATO's Development of Cross-border Cyber Defense Policy and Coordination

NATO forecasted today's cyber threat environment in 2010: "Cyber attacks are becoming more frequent, more organized and more costly [...]; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability."[6] NATO faces a cyber threat landscape that abounds with hackers, hacktivists, nation-states, and criminals. NATO itself has been targeted directly by Russian hackers seeking information on its defensive posture against Russia.[7] Furthermore, the recent attack by Russia on the Ukrainian power grid underscores the fact that Russian cyber attack capabilities are very real.[8] NATO also faces the same types of cyber breaches that affect businesses in America on a daily basis, ranging from random criminal acts to infiltrate NATO's systems to those of a more sophisticated, targeted nature. Despite preventive measures, cyber criminals around the world continue to gain access to these networks, including those that are classified.[9] In all, the current threat environment embodies much more significant risks than those first exemplified by the Russian cyber attacks on Estonia in

2007, which initially prompted NATO to address the dangers of cyber warfare.

How did NATO get to its current state in cybersecurity? NATO has always defended its military communication networks; however, during the 2002 Prague Summit, NATO stated that cyber defense was also part of its agenda and that it would strengthen its "capabilities to defend against cyber attacks."[10] The Prague Summit paved the way for NATO's creation of the NATO Computer Incident Response Capability (NCIRC) in 2002. Following the cyber attacks against Estonia in April and May of 2007, NATO issued its first "Policy on Cyber Defence" in January 2008. It later issued its "Strategic Concept" in 2011, as well as a newly enhanced cyber defense policy in 2014[11] in which NATO clarified that Article 5 could be invoked for a major digital attack.[12] It also pledged to improve cyber defense education, training, and exercise activities, in addition to its commitment to create a NATO cyber range capability.[13]

While NATO does not have a standing cyber defense force per se, its structures now cover the political, operational, and technical challenges of cyber defense. The North Atlantic Council (NAC), established under Article 9 of the North Atlantic Treaty, is the key entity within the Alliance that decides whether NATO responds to an attack of any nature. The Cyber Defence Committee (CDC), known as the Defence Policy and Planning Committee until 2014, is a senior advisory body that advises the NAC on cyber issues, as does the Cyber Defense Management Board (CDMB). Cyber is part of the NATO defense planning process that sets force goals for the Alliance as a whole.[14]

In 2012, NATO officials created the NATO Communication and Information Agency (NCIA) through a merger of a number of existing agencies.[15] The NCIA acts as NATO's principal deliverer of communications, command, and control (C3), which includes IT support to NATO Headquarters, the NATO Command Structure, and NATO Agencies. NCIA is responsible for defense capability planning; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture, exercises, and training; and acquisition and procurement of advanced technology. NCIA also functions as NATO's first line of cyber defense and houses both the NCIRC team and NATO's Information Security Operations Centre.[16]

Though formally outside of the NATO command structure, the Alliance also relies on work done by the NATO Cyber Defence Center

Nimmak

The 2015 hack of the Ukrainian power grid left over 230,000 residents without power and represented a new era in cyber attacks.

of Excellence (CCD COE) in Tallinn, Estonia. The CCD COE develops doctrinal and legal concepts, conducts training and exercise programs, carries out technical research and experimentation, and contributes to national and NATO capabilities.[17] The CCD COE launched the Tallinn Manual process, which has become the main authority on the applicability of the law of armed conflict to cyberspace. The Tallinn Manual 2.0 will be published in 2016 and will examine international law for cyber operations below the threshold of armed conflict.

NATO, much like the U.S. Government, is intensifying its relationships with private-sector cyber security companies. The NATO Industry Cyber Partnership (NICP) initiative is designed to encourage relationships with industry.[18] NATO is also developing a Cyber Rapid Reaction Team (RRT)[19] to protect its critical infrastructure, much like U.S. Cyber Command's Cyber Protection Teams (CPTs).[20] The protection of critical infrastructure under some circumstances may require offensive cyber capabilities to stop an attack. Unlike U.S. Cyber Command, NATO does not have an inherent offensive capability.

Finally, NATO is actively exercising its cyber forces. Cyber Coalition, a primarily table-top exercise, now includes more than 35 participating countries and has been integrated into NATO's crisis management exercises.[21]

In addition, the NATO CCD COE organizes the world's largest international live-fire cyber defense exercise in Tallinn,which in its 6th iteration in 2016 saw more than 550 people and over 26 nations participate.[22] Using a fictional scenario and virtualized networks, the exercise involved defenders, attackers, and bystanders. Twenty blue ("friendly") teams, represented by 19 nations and the NCIRC, were tasked with maintaining networks and services in a fictional country that was under attack.[23]

NATO's trend toward increased cooperation and joint operational exercises in the cyber realm tends to reflect a broader shift toward more robust coordination in the majority of its mission areas. NATO currently does not have any operational cyber capabilities as an organization, relying instead on Allied capabilities. The technical capabilities of NCIRC are used solely to protect the limited footprint of NATO's own command structure. As cyber defense becomes an operational domain in its own right, NATO should consider creating a tactical command similar to those for land, air, and maritime.[24] Given that cyber lends itself to economies of scale, NATO could also consider developing certain shared capabilities, similar to its strategic airlift and airborne warning and control systems capabilities.

The Increasing Influence of the EU in Creating a Single European Approach to Cyber Security

NATO's main efforts, however, remain focused on military defense. The organization has recognized the importance of civilian networks and the risks they face, particularly through its work on hybrid threats, but it does not have the legal or policy levers to address many of these questions directly. This is where the European Union comes in. The EU has superseded or supplemented member state policies in many areas, including those related to economic, justice, and home affairs. Accordingly, a large portion of Europe's legal environment consists of or is based upon EU legislation. While national governments guard their sovereignty in the areas of defense and foreign

policy, the EU maintains some limited authority in these areas. In fact, the EU is developing a considerable role in shaping the European cybersecurity landscape, primarily through legislation and expenditures related to economic regulation, individual rights, and internal security. Developments over the last 5 years have broadly paralleled the work of the Obama administration and the U.S. Congress. Much of this progress on both sides of the Atlantic has been related to cybersecurity information and threat indicator sharing. For example, the Cybersecurity Information Sharing Act of 2015, President Obama's 2015 Executive Order 13691 on information sharing, and legislation that statutorily codified the National Cybersecurity and Communications Integration Center (NCCIC) seek to accomplish many of the same goals as Europe's directive on Network and Information Security (NIS). These regulations focus primarily on increasing the speed, regularity, and centralization of information sharing between the public and private sectors.[25] In spite of a modest EU mandate with respect to foreign and defense policy, the EU has begun to play a substantial role in shaping the foreign policies of its member countries and the global cyber environment.

The EU has treated information security as a serious concern for some time, primarily through the lenses of data protection and regulation of the telecommunications sector. The 1999 Directive on Data Protection harmonized EU national rules on data protection, and also prohibited governments from discriminating against companies in other EU states on grounds of data protection. The 2002 regulatory framework on telecommunications[26] and directive on e-privacy[27] established security requirements for internet service providers and other telecommunications service providers, including reporting requirements for cyber incidents. One of the major motivations for European rules on security was to prevent different national rules on the matter from obstructing trade in services within the EU.

In 2004, the EU established ENISA, the European Network and Information Security Agency.[28] The relatively small agency, located in Greece, initially focused on research and training, but has been moving in a more operational and regulatory direction. ENISA operates Europe's bi-annual table-top cyber training exercise, Cyber Europe, which has nearly 300 public- and private-sector participating organizations.[29] Increasingly, ENISA is also taking on a regulatory role in aggregating the security incident reports submitted as part of EU regulation.[30] Further, in 2010, the EU decided to set up the European Union Computer Emergency Response Team (CERT-EU), a security team that, like the NATO NCIRC, focuses only on the security of EU institutions[31], though CERT-EU is quite active in various international cooperation networks. The EU has recently begun to work more intentionally and consistently to tackle cyber crime. While EU law has covered fraud and counterfeiting of non-cash payments since 2001[32], its legislation in this decade has focused on combatting child pornography and sexual exploitation online (2011) and harmonizing criminal penalties more broadly for cyber crime (2013).[33] Borne out of the 2010 European Commission's Internal Security Strategy[34], Europol launched the European Cybercrime Centre (EC3), which focuses on organized cybercrime, payment fraud, high-tech crimes, child sexual exploitation, and

cybercrimes or attacks that target critical infrastructure.[35]

In spite of a patchwork of pre-existing activity and legislation, the EU did not adopt a cross-cutting strategy until 2013. The EU's cybersecurity strategy, titled "An Open, Safe and Secure Cyberspace," covers the major aspects of a comprehensive approach to cyber defense and security.[36] The European Commission proposed new legislation covering cybersecurity of critical infrastructure, cooperation between national CERTs, and increased support for exercises and security research. It also launched a number of soft initiatives, including the dedication of a European cybersecurity month, making progress on cyber crime cooperation and mutual legal assistance, setting strategic goals for the newly created European Cybercrime Center, and completing the Europe-wide adoption of the Council of Europe's Convention on Cybercrime. The cyber strategy called for an international cyberspace policy based on the EU's core values, particularly those dealing with the promotion of fundamental rights, free expression, and a norms-based international legal order. The EU also addressed the cybersecurity of its military missions, while engaging with academia and industry to develop the European cyber industry and to protect the cyber security of the EU's own institutions. These priorities broadly mirror those announced by the Obama administration in the same year as part of the National Strategy to Secure Cyberspace.[37] Overall, the EU strategy has been successful, with action being taken to achieve its objectives. Still, a review of the state of play will reveal that much work remains.

Legislative accomplishments have had the most significant effects on Europe's cybersecurity policy landscape. Two new pieces of legislation will shape the basic legal framework for European cybersecurity once policymakers formalize them this summer after years of negotiation. First, the directive on Network and Information Security will require all governments to implement cybersecurity rules (including mandatory reporting for incidents affecting service availability) for their operators of essential services. This will effectively cover critical infrastructure in the fields of energy, transportation, telecommunications, medicine, and finance. This directive, however, will not create a central European inventory of critical infrastructure or require common standards. Cloud services, e-commerce marketplaces, and search engines will be subject to more specific and consistent European rules. National governments are required to cooperate and share some information, but the directive falls short of the mandatory Europe-wide cooperation and information-sharing mechanisms originally envisioned.

Difficulties in agreeing to rules governing the cybersecurity of critical infrastructure reflect the different national arrangements within member states of the EU. Some governments, including Germany and the Netherlands, treat cybersecurity as a question of homeland security, while others, such as Latvia and Denmark, consider it a question of defense. Still other countries, including Finland and Italy, see cybersecurity as a matter of commerce and communications. While many governments see the value of a strong pan-European approach, others view any central regulation of cybersecurity to be encroaching on their sovereignty. Nevertheless, these rules represent a sea change: EU law previously contained almost no clauses that sought to harmonize regulations on the protection of

critical infrastructure, which policymakers previously considered to be a purely national question. However, the use of such stark dividing lines is no longer feasible when infrastructures themselves span national borders.

The second major piece of new legislation is a new set of EU rules on data protection, the General Data Protection Regulation and law-enforcement specific rules in the Data Protection Directive.[38] The EU Charter of Fundamental Rights explicitly names the right to the protection of personal data alongside rights to human dignity, life, liberty, and privacy. There has been some form of EU data protection law in place since 1999.[39] The new regulation creates a consistent, single set of rules for all companies operating in the EU that handle the personal data of EU citizens, though these rules will also be complex and, in some cases, costly to implement. EU law protects individual rights that U.S. law does not explicitly consider, including the right to access information on how businesses are processing one's data, the right to transfer this data to other service providers, and the "right to be forgotten," which requires businesses to delete certain personal data on individuals upon their request. EU citizens will also benefit from data breach notification standards that are generally similar to those implemented in the United States. Fines for businesses that fail to comply with the Data Protection Regulation can rise to four percent of that company's global revenue.[40] Thus, while this data protection regulation is not explicitly about cybersecurity, it will create strong incentives for companies to implement good data governance practices and shore up

Security & Defense Agency

Members of the Security and Defense Agency, a major contributor to EU and NATO policy, meet in 2012 to discuss the intersection between public and private partnerships in the cybersecurity sphere.

measures that protect data integrity and confidentiality.

The headlines on European data protection have come not from the legislature, but from the courts: the European Court of Justice (the EU's supreme court) has taken an active role in striking down legislation it considers to be in violation of data protection rules. The court invalidated an EU directive on data retention that had required telecommunications companies to retain user data and share this with law enforcement if legally requested.[41] Furthermore, the court annulled the EU's data safe harbor scheme, which allowed private companies to transfer the personal data of European citizens that they possessed to servers located in the United States. This forced the United States and the EU to develop a new arrangement, called Privacy Shield, which acts as an "umbrella agreement" with the U.S. government. The renegotiation of safe harbor was aided by America's passage of the Judicial Redress Act, which gives EU citizens legal standing to sue the U.S. government for misuse of their personal data.[42] Furthermore, the "right to be forgotten," which is now enshrined in the recent data protection legislation, was initially created by a court decision in 2014.[43]

Operational cooperation among European governments has improved, with EU structures playing a growing role. The EU's best performance has been in the area of cyber crime, where cooperation among national cyber crime units and prosecutors has become frequent and close. The legal framework for cooperation on cyber crime is comparatively robust. The 2013 Directive on attacks against information systems includes a requirement for member states to respond to urgent requests within 8 hours. In 2013, EU member states also agreed to use an existing mutual evaluation mechanism to conduct thorough peer reviews of national cyber crime units.[44] Europol, Eurojust (the EU's agency for cooperation on prosecutions), and ENISA all have roles in cooperation with national authorities.

Europol's cyber crime center, the EC3, has become a hub for coordinating international and cross-sector support for joint law enforcement operations related to cyberspace. The EC3 is able to assist member states, as well as international law enforcement, in fighting cybercrime by leveraging Europol's infrastructure and network to share intelligence and align international priorities.

Europol, through the EC3, has facilitated and participated in numerous operations with U.S. law enforcement to disrupt cybercrime.[45] It has cooperated with the FBI and U.S. private sector partners like Microsoft and Symantec to take down some of the highest-profile botnets in recent years.[46] Such counter-botnet operations have involved up to 30 members, and often rely on the facilities and coordinating capabilities of Europol.[47] Pilot initiatives hosted by the EC3 (such as the Joint Cybercrime Action Task Force, which includes the FBI) are leading to multinational investigations and operations conducted jointly along every step, from identification of priorities to execution.[48]

Yet room for improvement remains. There is no single European contact for reporting cyber crime, and cross-border access to data necessary for cyber crime investigations has become more difficult following recent court judgments.[49] Europol reports that the invalidation of EU data retention rules has actively hampered investigations in areas such as computer intrusion, hacking, and child abuse[50],

and the decision has created legal uncertainty[51] around law enforcement access to cloud data.[52]

CERT cooperation has not developed as well as cybercrime cooperation. It has remained focused on bilateral and broader multilateral groupings, as well as narrower European groupings that include only some EU countries, such as the European gov-CERT group.[53] Notably, the CERTs that belong to this group do not have any membership from the countries that have joined the EU since 2004. The NIS directive now creates a format for cooperation among national CERTs, but this lacks the robustness of EU mechanisms for cyber crime cooperation. Information sharing and cooperation on incidents remain voluntary, so it will be up to member countries to make a push for closer cooperation.

The EU continues to face challenges in living up to its potential as the facilitator of a single market, which has stymied the growth of the European private sector's much-needed contribution to cybersecurity. Cybersecurity has not become the kind of big business in Europe that it currently is in the United States. While estimates vary, Europe constitutes at most one-quarter of the global cybersecurity market, and its cyber exports fall short of those of the United States and Israel. The U.S. federal government's cyber spending dwarfs that of national markets in Europe[54], and Europe's cyber insurance market is still nascent relative to that of the United States.[55] More fundamentally, European businesses have been reluctant to move toward using cloud services of all types, including those related to security.[56] In 2016, the EU plans to launch major initiatives to promote industrial policy and standardization in cybersecurity, including a 500 million euro public-private partnership to focus EU spending on research and development.[57] Part of the current challenge is market fragmentation. Not only does Europe lack a single purchaser like the U.S. federal government, but it also suffers from different private sector expectations and standards in individual countries. For example, a cybersecurity firm must apply for government contracts with 28 separate EU countries, each of which will have its own priorities and objectives for such contracts on top of their differing regulatory regimes. This situation increases transaction costs and complicates service provision to the extent that it is relatively growth prohibitive with respect to European cybersecurity firms that rely on government contracts.

The EU is also expanding its activity in specific sectors by applying its existing sectoral regulatory power and influence. Recently announced initiatives include further rules and information-sharing platforms and guidelines for the electricity, transportation, and finance sectors to set up several sector-specific Information Sharing and Analysis Centers (ISACs) and CERTs.[58]

In the global arena, the EU has used its modest authority to coordinate foreign policy to great effect in creating coherent "cyber diplomacy." In early 2015, EU governments formally endorsed a common position on major cyber foreign policy questions[59], but this approach has long been visible in bilateral cyber dialogue with numerous partners, including China, India, South Korea, and Japan.[60] Dialogue with the United States has helped the two entities coordinate a common approach to cybersecurity policy in most key areas.[61] Furthermore, the EU has prepared common policy positions for the diplomatic services of national governments to use when negotiating on a bilateral level.[62] The EU has

also allocated significant funding for cyber capacity building in third-party countries.

Since applying sanctions against Russia for its annexation of Crimea in early 2014, the EU has increasingly looked for ways to use its economic clout as a tool of diplomatic deterrence. The current president of the EU Council of Ministers has proposed that the EU apply naming and shaming, diplomatic and economic sanctions, as well as aggressive law-enforcement activity in the case of state-sponsored coercive cyber operations.[63] These measures would still be tame in comparison to U.S. activity, but constitute a significant step forward from otherwise loosely coordinated EU action in this area.

In the core defense area, the EU's ambitions have been more modest than NATO's, but it has put in place a policy framework for cyber defense with a roadmap that policymakers review every 6 months. This framework includes measures that support the development of national cyber defense capabilities, protect command and control and communications networks, improve training and exercises, and ensure coherence between EU and NATO efforts.[64]

The Future of EU-NATO and EU-U.S. Cooperation

EU-NATO cooperation has always presented a challenge due to the differences in the makeup of each organization's membership. There are signs that the relationship could be warming up: the EU and NATO signed a technical arrangement in February 2016 to increase information sharing between the NCIRC and CERT-EU.[65] The agreement authorizes technical information sharing to improve incident prevention, detection, and response, and is similar to U.S. information-sharing requirements between government agencies. While information sharing within the American federal government has been ongoing since 2004[66], it is now becoming more effective than ever due to improvements in information-sharing software, hardware, and procedures, and the adoption of standard technical specifications. Furthermore, two non-NATO EU countries are members of the CCD COE, and the EU and non-NATO members participate in or observe various NATO-related cyber exercises.

Ultimately, the United States and Europe would benefit from an EU-NATO-U.S. triangle, where the Allies could work together within NATO to further develop joint cyber defense capabilities and approaches. The EU and the United States could simultaneously work bilaterally to achieve shared objectives on other cybersecurity matters. A joint policy agenda between these two powers could include convergence between EU and U.S. security standards for cyber products and services, including joint procurements in less sensitive areas; collaborative exercises; more structured information sharing; continued development and elevation of international cyber crime law enforcement regimes; and consistent and practical data protection regulations.

The United States has much to contribute to the cyber operations of NATO and the EU, and can serve as a force to bring these two organizations closer together. American law enforcement and the deep cybersecurity talent reserves of its private sector have already proven to be invaluable partners in Europol's cyber crime investigations. The trend toward globalized impacts from cyber threats makes it likely that partnerships on matters of law enforcement and cybersecurity in general will continue to grow. A few areas in which the

United States, NATO, and the EU could further cooperate on cybersecurity policy include combined cyber forensics training to improve attribution, more widespread support for resilience and remediation practices, and greater coordination between the U.S. and EU judicial regimes when it comes to bringing cybercriminals to justice.

Although the cybersecurity threat has been growing for the past two decades, the preference of national governments for sovereignty in the realms of foreign and defense policy has traditionally limited the cybersecurity ambitions and organizational capacity of both NATO and the EU. It was not until approximately 6 years ago that European policymakers began to recognize that the threat from cyber attacks and cyber crime is inherently a cross-border problem that requires cross-border solutions. With increasing support from the European states that belong to NATO and the EU, these international entities have been able to build out their organizational and operational structures and capacities.

The EU and NATO have respectively made tremendous progress in building their capacity to coordinate cybersecurity and defense activities among their members. The increasing willingness on the part of these organizations to work more closely with one another and international partners is also a promising, if recent, development. Europol's multilateral law enforcement operations against cybercriminal groups and forums represent one of the best emerging models for international resource pooling and operational coordination. In fact, the crucial role that international law enforcement must play in combatting the global cyber

National security Agency

Cooperation with U.S. organizations like the National Security Agency (headquarters pictured above) and the well-developed American private sector have already improved NATO and EU cyber operations, but further integration must occur to address effectively the cyber challenge.

threat qualifies entities such as Europol for a more elevated role in international diplomacy. However, cyber crime is only one piece of the larger puzzle of cybersecurity and cyber defense. The recent successes of coordinated law enforcement operations will reach their full potential for positive impact only if NATO and the EU apply lessons learned from that realm to broader cyber policy issues.

Overall, the cyber threat landscape is pushing national governments and international organizations toward greater transatlantic security cooperation. With a growing cyber threat from nation-state actors, including a resurgent Russia, and a new norm of conflict that ensures kinetic operations will be paired with cyber aggression for the foreseeable future, security cooperation in Europe and around the world is increasingly necessary. The strides that NATO and the EU have made thus far to address cyber threats are promising but ultimately only foundational. These organizations must build on this foundation by continuing to make progress toward cross-border integration of information, capabilities, and defensive strategies if the advantage in cybersecurity is ever to be wrested from the attacker.

PRISM

Notes

[1] "Estonia Hit by 'Moscow Cyber War'," *BBC News*, May 17, 2007, <http://news.bbc.co.uk/2/hi/europe/6665145.stm>.

[2] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, <smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>.

[3] Statement of Frank J. Cilluffo, "Testimony on Emerging Cyber Threats to the United States," testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, U.S. House of Representatives, February 25, 2016.

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

[5] Statement of Frank J. Cilluffo, "Testimony on Emerging Cyber Threats to the United States," testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, U.S. House of Representatives, February 25, 2016.

[6] "Active Engagement, Modern Defence: Strategic Concept for the Members of the North Atlantic Treaty Organisation," North Atlantic Treaty Organization, November 19, 2010, <http://www.nato.int/cps/en/natolive/official_texts_68580.htm>.

[7] Kenneth Geers, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," *NATO CCDCOE Publications*, 2015, <https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Weedon_08.pdf>.

[8] Sean Adl-Tabatabai, "FBI War of Cyber Attack on Electrical Grid," April 11, 2016, <http://yournewswire.com/fbi-warn-of-cyber-attack-on-electrical-grid/>.

[9] "The History of Cyber-attacks – a Timeline," *NATO Review Magazine*, <http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>.

[10] "NATO Prague Summit Declaration – Press Release," North Atlantic Treaty Organization, November 21, 2002, <http://www.nato.int/docu/pr/2002/p02-127e.htm>.

[11] "Wales Summit Declaration," North Atlantic Treaty Organization, September 5, 2014, <http://www.nato.int/cps/en/natohq/official_texts_112964.htm>.

[12] Steve Ranger, "NATO updates cyber defense policy as digital attacks become a standard part of conflict," *ZDNet*, June 30, 2014, <http://www.zdnet.com/nato-updates-cyber-defence-policy-as-digital-attack>.

[13] "A cyber range is a virtual environment that is used for cyberwarfare training and cybertechnology development. It provides tools that help strengthen the stability, security and performance of

cyberinfrastructures and IT systems used by government and military agencies. Cyber ranges function like shooting or kinetic ranges, facilitating training in weapons, operations or tactics." See: "Cyber Range," *Techopedia*, <https://www.techopedia.com/definition/28613/cyber-range>.

[14] "The NATO Defence Planning Process," North Atlantic Treaty Organization, November 11, 2014, <http://www.nato.int/cps/en/natohq/topics_49202.htm>.

[15] These agencies include: NATO Consultation, Control and Command Organisation; NATO Communication and Information Systems Services Agency (NCSA); NATO Consultation, Command, and Control Agency (NC3A); NATO Air Command and Control System Management Agency (NACMA); and the NATO Headquarters Information and Communication Technology Service (ICTM).

[16] "NATO Communications and Information Agency," North Atlantic Treaty Organization, April 7, 2016, <http://www.nato.int/cps/en/natolive/topics_69332.htm>.

[17] "About Cyber Defense Centre," NATO Cooperative Cyber Defense Centre of Excellence, 2016, <https://ccdcoe.org/about-us.html>.

[18] "Cyber Defence," North Atlantic Treaty Organization, February 16, 2016, <http://www.nato.int/cps/en/natohq/topics_78170.htm>.

[19] James A. Lewis, "The Role of Offensive Cyber Operations In NATO's Collective Defence," *Tallinn Paper*, No. 8, 2015, <https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf>.

[20] Collin Wood, "U.S. Cyber Command Launches 13 New Cyber Protection Teams," *Government Technology*, December 16, 2016, <http://www.govtech.com/security/US-Cyber-Commands-Launches-13-New-Cyber-Protection-Teams.html>.

[21] "Cyber Exercise Challenges Defence," North Atlantic Treaty Organization, November 20, 2015, <https://www.shape.nato.int/cyber-exercise-challenges-defense>.

[22] "Exercise Locked Shields 2016 Highlights Priorities in Cyber Defence," Cooperative Cyber Defence Centre of Excellence, April 21, 2016, <https://ccdcoe.org/exercise-locked-shields-2016-highlights-priorities-cyber-defence.html>.

[23] The U.S. conducts similar live-fire exercises throughout the year, including Shreiver War Games, Cyber Guard, and Cyber Shield in addition to others. Typically, U.S. Military Forces use either the DOD-owned National Cyber Range (NCR) or a privately operated commercial range to conduct training and exercises. Lockheed Martin operates the NCR and there are a few select privately owned commercial ranges, including SimSpace and Raytheon's Cyber Range with which to conduct training and exercises. U.S. commercial ranges such as SimSpace have ready-made red team attacks and scoring mechanisms to determine how well the cyberspace defenders fared against the adversary.

[24] See NATO command structure, "Military Command Structure," North Atlantic Treaty Organization, <https://www.shape.nato.int/military_command_structure>.

[25] Rita Tehan, *Cybersecurity Legislation, Hearings, and Executive Branch Documents*, (Washington, DC: The Congressional Research Service, March 30, 2016), <https://www.fas.org/sgp/crs/misc/R43317.pdf>; "Network and Information Security Directive," European Commission, March 16, 2015. <https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-nis-directive>.

[26] "Telecoms Rule," European Commission Digital Single Market, <https://ec.europa.eu/digital-single-market/en/telecoms-rules>.

[27] "2002 EU Data Protection Directive," European Parliament, July 12, 2002, <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/24eprivacy_2.pdf>.

[28] "About ENISA," European Union Agency for Network and Information Security, <https://www.enisa.europa.eu/about-enisa>.

[29] "Cyber Europe 2014," European Union Agency for Network and Information Security, <https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/ce2014>.

[30] "Incident Reporting," European Union Agency for Network and Information Security, <https://www.enisa.europa.eu/topics/incident-reporting>.

[31] "About Us," Computer Emergency Response Team, CERT-EU, <https://cert.europa.eu/cert/plainedition/en/cert_about.html>.

[32] "Council Framework Decision: Combating Fraud and Counterfeiting of Non-cash Means of Payment," Eur-Lex, May 28, 2001, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001F0413>.

[33] "Cybercrime," European Commission, Migration and Home Affairs, April 18, 2016, <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm>.

[34] "EU Internal Security Strategy," Eur-Lex, November 22, 2010, <http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=uriserv:jl0050>.

[35] "Combatting Cybercrime in a Digital Age," Europol, 2016, <https://www.europol.europa.eu/ec3>.

[36] "Joint Communication to the European Parliament, the Council, The European Economic and Social Committee, and the Committee of the Regions," European Commission, February 7, 2013, <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf>.

[37] "Cybersecurity," The White House, Foreign Policy, <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity>.

[38] "Protection of Personal Data," European Commission, Justice, <http://ec.europa.eu/justice/data-protection/>.

[39] "Directive 95/46/EC of the European Parliament and of the Council," The European Parliament and the Council of the European Union, October 24, 1995, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>; for information on when EU member states adopted related provisions see: "Status of Implementation of Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data," European Commission, <http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm>.

[40] Chloe Green, "The EU General Data Protection Regulation is now Law: Here's What you Need to Know," *Information Age*, January 28, 2016, <http://www.information-age.com/technology/data-centre-and-it-infrastructure/123460854/eu-general-data-protection-regulation-now-law-heres-what-you-need-know>.

[41] "European Union: ECJ Invalidates Data Retention Directive," Library of Congress, June 2014, <https://www.loc.gov/law/help/eu-data-retention-directive/eu.php>.

[42] "Questions and Answers on the EU-US Data Protection 'Umbrella Agreement,'" European Commission, September 8, 2015, <http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm>; Eric Geller, "Everything You Need to Know About the Big New Data-privacy Bill in Congress," *The Daily Dot*, February 4, 2016, <http://www.dailydot.com/politics/what-is-the-judicial-redress-act-europe-data-privacy-bill/>.

[43] "Factsheet on the 'Right to be Forgotten' Ruling," European Commission, <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>.

[44] "Seventh Round of Mutual Evaluations – Order of Visits and Observers," The Council of the European Union, March 25, 2014, <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%207940%202014%20INIT>.

[45] Margarita Louca, "Successful Botnet Takedowns: the Good Cooperation Part, Europol European Cybercrime Center," European Cybercrime Center, <https://www.botconf.eu/wp-content/uploads/2015/12/OK-K01-Margarita-Louca-Botnet-takedowns-cooperation.pdf>.

[46] These botnet takedowns include those affecting: ZeroAccess (2013), Gameover ZeuS (2014), Ramnit (2015), Beebone (2015), and Dorkbot (2015). These takedown operations collectively disconnected millions of computers from the command and control infrastructures of malicious botmasters who used them to commit extensive financial fraud, distribute ransomware, and launch DDoS attacks, among other things.

[47] "International Takedown Wounds Gameover ZeuS Cybercrime Network," *Symantec Official Blog*, June 2, 2014, <http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network>.

[48] "Joint Cybercrime Action Taskforce (J-CAT)," Europol, 2016, <https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat>.

[49] See Europol's guidelines for reporting a cyber crime in Europe: "Report Cybercrime," Europol, 2016, <https://www.europol.europa.eu/content/report-cybercrime>.

[50] "Appendix 2: An Update on Cyber Legislation," Europol, <https://www.europol.europa.eu/iocta/2015/app-2.html>.

[51] "Criminal Justice Access to Data in the Cloud: Challenges," Council of Europe Cyber Convention Committee, May 26, 2015, <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf>.

[52] The European Commission has stated it will not propose new legislation following the court's judgment, instead leaving the question to national governments, <http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm>.

[53] For a complete list of the EU Certs that belong to the ECG, see: "European Government CERTS (ECG) Group," ECG Group, <http://www.egc-group.org/contact.html>.

[54] Steve Morgan, "Cybersecurity Market Reaches $75 Billion in 2015; Expected to Reach $170 Billion by 2020," *Forbes*, December 20, 2015, <http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#180752712191>; "Cybersecurity Market Report," *Cybersecurity Ventures*, Q3 2015, <http://cybersecurityventures.com/cybersecurity-market-report-q3-2015/> ; "Commissioner Oettinger Receives the Final Report of the European Cybersecurity Industrial Leaders," European Commission Digital Single Market, January 25, 2016, <https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders>.

[55] Friedrich Geigger, "Cyber Insurance Demand said Rising in Europe," *The Wall Street Journal*, January 28, 2015, <http://blogs.wsj.com/digits/2015/01/28/cyber-insurance-demand-said-rising-in-europe/>.

[56] Konstantinos Giannakouris and Maria Smihily, "Cloud Computing – Statistics on the Use by Enterprises," Eurostat, November 2014, <http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises>.

[57] "Cybersecurity Industry," European Commission, April 12, 2016, <https://ec.europa.eu/digital-single-market/node/80873>.

[58] "Security: EU Strengthens Response to Hybrid Threats," European Commission, April 6, 2016, <http://europa.eu/rapid/press-release_IP-16-1227_en.htm>.

[59] "Council Conclusions on Cyber Diplomacy," February 11, 2015, <http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf>.

[60] "Cyber Diplomacy: EU Dialogue with Third Countries," European Parliament Think Tank, June 29, 2015, <http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)564374>.

[61] "Joint Elements from U.S.-E.U. Cyber Dialogue," US Department of State Office of the Spokesperson, December 8, 2015, <http://www.state.gov/r/pa/prs/ps/2015/12/250477.htm>.

[62] For example: "World Summit on the Information Security," Council of the European Union, May 29, 2015, <http://www.statewatch.org/news/2015/jun/eu-council-wsis-review-lines-to-take-9334-15.pdf >.

[63] "Developing a Joint EU Diplomatic Response against Coercive Cyber Operations," Council of the European Union, February 9, 2016 <http://data.consilium.europa.eu/doc/document/ST-5797-2016-INIT/en/pdf>.

[64] "EU Cyber Defence Policy Framework," Council of the European Union, November 18, 2014, <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf>.

[65] "EU and NATO Increase Information Sharing on Cyber Incidents – Press Release," European External Action Service, February 10, 2016, <http://eeas.europa.eu/statements-eeas/2016/160210_01_en_en.htm>.

[66] Veronica Chinn, Lee Furches, and Barian Woodward, "Information-Sharing with the Private Sector," *Joint Force Quarterly* 73, April 1, 2014, <http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/577502/jfq-73-information-sharing-with-the-private-sector.aspx>.

Photos

Photo 126. Photo by Colin. 2013. Backlit keyboard. From <https://commons.wikimedia.org/wiki/File:Backlit_keyboard.jpg >. Licensed under Creative Commons Attribution-ShareAlike 4.0 International <http://creativecommons.org/licenses/by-sa/4.0/>. Photo unaltered.

Page 129. Photo by Nmrmak. 2010. Power Grid. From <https://www.flickr.com/photos/51392234@N06/4939340032/in/album-72157624835170622/>. Licensed under Creative Commons Attribution 2.0 Generic License <https://creativecommons.org/licenses/by/2.0/legalcode>. Photo unaltered.

Page 133. Photo by Security & Defense Agency. 2012. Public-private cooperation in cyber-security. From <https://www.flickr.com/photos/securitydefenceagenda/6801269269/in/album-72157629215245689/>. Licensed under Creative Commons Attribution 2.0 Generic License <https://creativecommons.org/licenses/by/2.0/legalcode>. Photo unaltered.