BUILDING COMMON GROUND IN TRANSATLANTIC CYBERSECURITY
A Baltic Approach
By Eriks K. Selga
ABOUT CEPA

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

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

Mobile phones are seen during the Locked Shields, cyber defence exercise organized by NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia April 10, 2019. REUTERS/Ints Kalnins
Contents

About the Authors ................................................................. 2
Acknowledgments .................................................................. 2
Executive Summary ............................................................. 3
Introduction ............................................................................ 4
Data Architecture .................................................................. 6
Data Protection ...................................................................... 8
Law Enforcement Cooperation ............................................. 9
Cyberwarfare ....................................................................... 11
Divergent Cybersecurity Frameworks .................................... 12
Cybersecurity Gaps .............................................................. 14
Recommendations ............................................................... 15
Endnotes .............................................................................. 17
About the Authors

Ēriks Selga is a Digital Innovation Baltic Fellow with the Transatlantic Leadership team. Ēriks is a Visiting Researcher at the Latvian Institute of Foreign Affairs, Associate Scholar at the Foreign Policy Research Institute, and a current Ph.D. Candidate at the University of Hong Kong Faculty of Law, where he is studying the intersection of law and innovation in the context of FinTech and other datafication trends. Ēriks holds a Master’s degree in International Law from Temple Beasley School of Law. Ēriks research will focus on data governance in the transatlantic space and will explore how NATO has adapted to transatlantic digitization.

Acknowledgments

This program is made possible by funding from the Baltic-American Freedom Foundation (BAFF). For more information about BAFF scholarships and programs, visit www.balticamericanfreedomfoundation.org.

The views expressed by the author are their own and do not represent the views of BAFF.
Executive Summary

• As sectors continue to grow more dependent on data flows, cybersecurity threats are becoming a bigger priority for the United States and the European Union (EU). Preventing cybersecurity breaches is becoming increasingly important to critical sectors and critical functions across the transatlantic.

• Data governance frameworks between the United States and the EU diverge significantly, with fundamental differences in approaches to data architecture, data protection, law enforcement data sharing, cyber interventions, and cybersecurity frameworks.

• Differences in data governance lead to growing cybersecurity risks in the transatlantic, caused by different cybersecurity risk assessments, cybersecurity incident reporting standards, and information sharing networks.

• The Baltic approach ensures that all cybersecurity information funnels through a forum of all relevant public, private, military, and civilian sector stakeholders.

• By establishing an international cybersecurity council for critical functions, the United States and the EU set a shared scope for threat collection, and a forum for sharing threats.

• Cybersecurity coordination should be advanced as a priority under the U.S.-EU Trade and Technology Council working groups.

• Civilian and military cybersecurity expertise and capacity should be conflated. The EU proposal for a Joint Cyber Unit would establish a unit that can become a European representative to the United States.
Introduction

Most sectors in the transatlantic alliance are quickly becoming digital, growing increasingly dependent on data flows to provide vital goods and services. As a consequence, the ambit of cyber risk is expanding proportionately, becoming increasingly costly.\(^1\) The Colonial Pipeline ransomware attack in May resulted in fuel shortages in several states and directly increased fuel prices.\(^2\) The SolarWinds supply chain attack, detected in December of 2020, targeted a third-party service provider, leaving vulnerable more than 18,000 entities worldwide, including U.S. agencies like the Department of Defense, the Department of Homeland Security, the State Department, as well as NATO systems, European government agencies, and Fortune 500 companies.\(^3\) In 2017, NotPetya erased the capital assets of hundreds of companies in minutes by encrypting and wiping their information technology systems with damages so costly they impacted national GDPs. These cyberattacks travelled across devices, sectors, jurisdictions, and oceans to ultimately inflict damage.

Cybersecurity is thus a growing priority. It is fast expanding in scope from protecting just critical infrastructure, like energy and finance, to protecting critical functions, like water distribution and payment processing, and increasingly the safety and stability of the structures and individuals underpinning them. The ambit of cyber threats is gradually creating a data complex that ties together the digital vulnerabilities of public, private, civilian, and military sectors. Yet, widening divergences in U.S. and European Union (EU) data governance approaches are limiting the interoperability of data between these sectors, directly impacting the ability of the alliance to counter the growing array of cyber risks.

The U.S. liberal market-based approach to data centers around data ownership rights, upholding a property-based regime where companies can process personal data by default.\(^4\) In turn, to extend the single market into the digital realm, the EU approach to data is focused on harmonizing data regimes between its 27 member states, generally through heavy-handed rights-based regulation.\(^5\) These differences in governance have extended into broader forks in the handling of data sharing architecture, personal data protection regimes, and digital intelligence orders.

Each bifurcation in data policy adds a layer of complexity to cybersecurity initiatives in the form of new technical standards, trust services, or supply chain certification considerations. However, the current transatlantic cybersecurity status quo is not yet equipped to handle the variance in data governance regimes. In the United States, the main cross-sectoral cybersecurity framework is created by the National Institute of Standards and Technology (NIST) in the form of a nonbinding set of best practices.
that companies can apply. On the other hand, the EU’s Network and Information Security Directive (NIS Directive) stipulates digital service providers operating across Europe enact mandatory cybersecurity frameworks. In such a scenario, the data of an international company that operates in both markets will travel through servers that may have fundamentally different cybersecurity frameworks, risk management systems, or incident reporting requirements.

Kept unaligned, these differences risk extending gaps between the cybersecurity efforts of the transatlantic partners, as well as creating new ones as new digital initiatives develop. Four working groups within the recently formed U.S.-EU Trade and Technology Council are dedicated to coordinating information and communications technology (ICT) and data governance challenges — an important indicator of the priority of digital governance and of the political will to find common ground. In this policy brief, the critical pain points for transatlantic cybersecurity cooperation are addressed, outlining rising divergences in data architecture, data protection regimes, law enforcement cooperation, and cyber interventionist capacity. After highlighting how these divergences create new cybersecurity gaps, the problem is addressed. The Baltic approach, characterized by a flexible governance structure, offers one model of how the transatlantic alliance can leverage data governance from the bottom up, toward a more integrated transatlantic data relationship.
Data Architecture

The first layer of U.S.-EU cyber frictions stems from differences in foundational data infrastructure. Public sector data stewardship frameworks in the United States are nascent and decentralized, with data generally being siloed separately in federal and state-level institutions. In 2017, the U.S. Commission on Evidence-Based Policymaking laid out a comprehensive strategy for expanding access to government data, enhancing privacy protections, and building capacity for evidence building in government. Half of the recommendations have been incorporated in the 2018 U.S. Evidence Act, which establishes new leadership roles in federal agencies like chief data officers, evaluations officers, and statistical officials. Title II of the 2019 OPEN Government Data Act also establishes data collection requirements for federal agencies, requiring them to define the data, methods, and analytical approaches used to acquire and facilitate the use of evidence in policymaking. The other half of the U.S. Commission on Evidence-Based Policymaking’s recommendations, including the creation of a national secure data service that would serve as a centralized standard channel for exchanging the collected data, is still a bill under discussion in the U.S. House of Representatives.

In contrast, the EU has launched a comprehensive data strategy that envisions consolidating enormous cross-sectoral data pools that would draw on both public and private sector data. The data pools will be built within the European Cloud Initiative, which will simplify access to data by making it possible to move, share, and reuse data seamlessly across European markets and borders. Together with the Franco-German GAIA-X initiative — a project to connect cloud providers around Europe, harmonize technical standards, and ensure data privacy and security walls — the EU is creating its own walled garden of data. Federated cloud initiatives are slowly creating partner networks via national GAIA-X hubs with unified data formats, quality standards, and security mechanisms that foster data sharing and interoperability among EU data spaces. This infrastructure also supports a well-developed EU electronic ID certification and trust services regime implemented under the eIDAS Regulation. The harmonized digital identity system standardizes access to a range of electronic transactions in the European single market.
The divergence in architecture provides a dual challenge. First, the European Cloud Initiative and GAIA-X set a heightened level of rules and standards for the transfer of data within the European single market — this aims to include encryption rules for privacy, internet protocols for interoperability, and trust services for transparency. With a goal of increasing EU “digital sovereignty,” it is not only a mechanism to keep information safe within the EU cloud bubble but also keep malign and uncertified entrants out. U.S. companies wishing to operate within the EU data garden will need to adapt to its standards and will potentially be required to share data into EU data pools. Second, the cloud infrastructure, trust service, and digital identity regime will push EU cybersecurity standards even higher, especially under the revised NIS Directive, to ensure mitigation of the growing data concentration risk.
Data Protection

Data protection is the clearest point of friction between U.S. and EU data policy. Data protection rules in the United States are only applicable to niche domains and differ across states, with enforcement undertaken by the Federal Trade Commission and self-regulation. Because of a relatively weak patchwork of data protection rules, the United States has repeatedly been deemed by European courts as being unable to ensure adequate protection of EU citizens' data. In 2016, the Court of Justice of the European Union (CJEU) ordered the shutdown of the Safe Harbor Program in the Schrems I judgment, and ordered the shutdown of the successor EU-US Privacy Shield regime in Schrems II in 2020. As a consequence, U.S. companies are prohibited from holding EU citizens' data in their domicile. The available remedies are standard contractual clauses (SCCs), which place a heavy burden on data exporters to enact and authorities to enforce.

Recently, the European Commission published the final version of new SCCs, increasing the threshold of adequacy. Parties aiming to secure adequacy must now, for example, assess compatibility with local laws regarding conflicting data protection rules, contract to pursue legal remedies against such requests, and ensure that onwards transfers are also consistent with SCCs. The SCCs also assess a company’s cybersecurity measures through 17 suggested categories of requirements.

Though the cloud infrastructure is internal to the EU, the differences in data protection are increasingly having an extraterritorial effect. Adequacy rules and SCCs require any external personal data that leaves for the United States to travel with protection. Among these protections is a slew of cybersecurity standards with which the party must ensure compliance. These standards are higher than the standards set by the NIST Cybersecurity Framework.
Law Enforcement Cooperation

This data protection regime is also exemplified in the increasingly difficult cooperation between law enforcement agencies for whom cross-border digital information sharing is becoming critical to performing investigations. A report found that more than 85% of investigations in the EU require electronic evidence, and in two-thirds of cases the evidence lies with online service providers in different jurisdictions.17

The frameworks for mutual sharing of relevant information historically have been negotiated directly between national governments, most importantly through the U.S.-EU mutual legal assistance treaty (MLAT) system. MLATs typically draw out the rules for cooperation on a range of law enforcement issues, such as locating and extraditing individuals, freezing assets, requesting searches and seizures, and taking testimony.18 Recently, this system has exemplified the lag between digital governance and the growth of globalized data and the expansion of cloud-based services and data storage.

Under the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, the U.S. government is authorized to compel production of communications content without regard to the location of the data if a warrant is issued. Though the CLOUD Act allows pursuing bilateral data-sharing agreements between the United States and partner countries to allow data to be obtained directly from companies located in the other country, the EU data authorities find that the CLOUD Act does not ensure sufficient data protection standards, and fundamentally contradicts EU rules.19 The EU’s General Data Protection Regulation (GDPR), for example, recognizes the decisions of foreign adjudicative or administrative authorities only if they are based on international agreements like MLATs, challenging the unilateral functionality of the CLOUD Act.20 In turn, the EU has begun drafting its own rules to shift toward direct cooperation with service providers via the E-evidence package, defining the scope, data types, procedures, and other factors for law enforcement cooperation.
The protections offered by the GDPR also apply to the direct and indirect exchange of data between governments for law enforcement purposes. The United States must generally now use MLATs to secure any data for an EU-linked investigation, precluding the direct access provided by the CLOUD Act through partner relationships like the one the United States has with the United Kingdom. For any follow-up to criminal investigations into cyber incidents, the schism in transatlantic access to digital evidence places obstacles to securing actionable information that could prevent further attacks.
Cyberwarfare

A fundamental difference between the United States and the EU is in their outward-facing cyber toolkits. The former pursues forward cyber engagement, while the latter practices defensive “cyber diplomacy.” The U.S. State Department and U.S. Department of Defense formulated the International Strategy for Cyberspace and the Strategy for Operation in Cyberspace which sets principles for the formation of cyber alliances and containment in cyberspace. The U.S. national defense strategy proclaims a “right to self-defense” in cyberspace, explicitly declaring the ability to block or control conflict escalation through network methods as a strategic objective. The United States practices “persistent engagement” with adversaries to disrupt malicious cyber activity at the source. For example, the United States openly reports the use of offensive cyber operations, like the implanting of malware in Russian power grids in 2019, to effect kinetic strikes and beckon disruption.

The EU, as an international organization, is not mandated to harmonize national security standards, which remain the sovereign rights of member states. Instead, EU data intervention is limited to its cyber diplomacy, a cyber-sanction regime through which targeted asset freezes or asset bans against individuals and concrete entities are carried out to prevent or discourage malicious cyberattacks that could have a significant impact on the EU. Only the Council of the European Union can take this decision, unless EU member states sanction individually. The first time the EU used the tool was against Russian, Chinese, and North Korean hackers involved in the “WannaCry” and “NotPetya” attacks.

The asymmetry in the use of cyber interventions is in part responsible for the broader paradigmatic difference in the mandatory cybersecurity standards of the EU versus the voluntary standards of the United States, but it also bolsters continued divergence. Through offensive operations, the United States gains access to a source of information that the defensive EU networks may have limited access to, unless shared via national channels with the Computer Emergency Response Teams (CERTs) of individual EU countries. Without standardized channels of intelligence exchange, the EU and the United States may work under the presumption of different risk models, harming collective cyber threat prevention capacity.
Divergent Cybersecurity Frameworks

The differences in data architecture, data protection and law enforcement data exchange, and cyber toolkits between the United States and the EU ultimately cycle back to two diverging cybersecurity frameworks that are asymmetrically building resilience. The Cybersecurity Framework created by NIST is, notably, a voluntary set of standards, guidelines, and best practices for organizations. The Cybersecurity Framework is considered best practice by organizations, but does not bind them. The Cybersecurity Information Sharing Act of 2015 (CISA) does not contain specific requirements for private entities to implement specific cybersecurity measures. It instead facilitates information sharing. Cyber incident reporting requirements apply to a narrow set of subjects, including contractors handling federal data. Only recently has CISA begun cataloging bad cybersecurity practices. Though a comprehensive cybersecurity bill failed to pass in the House in 2012, recent bill initiatives are being prepared to institute mandatory reporting requirements for critical U.S. infrastructure and cybersecurity requirements for devices connected to the Internet of Things network.

Under the EU’s NIS Directive, all member states and essential service operators should use the best measures to safeguard their systems and report incidents according to country-level risk thresholds. The 2018 EU Cybersecurity Act provides the EU Agency for Cybersecurity (ENISA) with a permanent mandate to maintain European cybersecurity certification frameworks and prepare technical grounds for certification schemes. These certification frameworks provide a comprehensive set of rules to evaluate and assure the cybersecurity risks of products, allowing for easier trade across borders. The upcoming NIS Directive 2 requires member states to ensure that operators of medium and large enterprises, essential services, and digital service providers implement cybersecurity requirements and report incidents. The European Commission’s proposal for the Digital Operational Resilience Act (DORA) aims to take cybersecurity even further by creating comprehensive rules for the financial sector, establishing an oversight framework for critical ICT third-party providers to subject entities, and information sharing among sector-specific cybersecurity threats. DORA is a prototype for an EU sectoral cybersecurity framework which is likely to be replicated in other sectors as well.
There is a significant imbalance in cybersecurity reporting requirements and subsequent cyber threat assessment capacity in EU and U.S. normative frameworks. Without being able to build on cyber incident reports, the U.S. cyber risk parameters may differ from those diffused within the EU. This will result in different levels of cybersecurity standards instilled under the NIS Directive and NIST Cybersecurity Framework regimes going forward, which will directly impact the ability to manage cyber risks across the United States and the EU member state.
Cybersecurity Gaps

Even as the NIS Directive sets their main functions, the nature of Computer Emergency Response Teams (CERTs) differ significantly across jurisdictions in the EU. CERTs can be tied to academic, civilian, military, or law enforcement structures, limiting their cooperation and the interoperability of their experiences. Their relationships are often based on trust, built from the ground up. At the EU level, these relationships channel through ENISA, which also carries out security risk assessments of critical ICT services, systems, and product supply chains. The European Commission coordinates this for specific risk factors and systems.

With the second NIS Directive adding further security and incident reporting requirements, transatlantic cybersecurity cooperation may be jeopardized by the increasing disparity in risk assessment coordination across the Atlantic. The scope of EU CERTs is evolving to meet different standards than that of U.S. partners. Within the EU federated cloud system, CERTs will also be responsible for ensuring the safety of trust services, and digital IDs, as well as the central bank digital currencies (CBDC) infrastructure which the European Central Bank (ECB) has undertaken to establish. The range of risks which EU and U.S. CERTs will cooperate in may continue to grow apart.

These divergences have a secondary impact under NATO’s dual use doctrine. The security of 5G, for example, is a growing priority for both civilian and military sectors. However, cooperation between the two increasingly overlapping arenas remains light. While the EU Cybersecurity Strategy aims to increase cooperation among both military and civilian CSIRTs, the United States is largely left out of this relationship, except through NATO or bilateral cooperation efforts.
Recommendations

The diverging data governance approaches of the United States and the EU require a flexible approach to cybersecurity that can react quickly, and across policy levels, to best incorporate and exchange security practices, build trust, and ultimately bolster resilience across the transatlantic space. The Baltic approach offers a model that can help form a dynamic cross-sectoral threat information sharing feedback loop. In Latvia, for example, the Digital Transformation Guidelines establish an Information Society Council that meets with stakeholders from the private, public, military, and civilian sectors at the highest executive level to directly exchange digital threat information. As sectors become more dependent on data flows, the Information Society Council can dynamically react to changes in threats. The following recommendations draw on the Baltic experience to expand channels for the United States and the EU to find common ground for realignment across divergent data governance and cybersecurity regimes. These channels may be helpful in lessening divergences in practical cyber threat aversion, and may aid in normative alignment.

Establish and Advance National Cybersecurity Councils for Critical Functions

National cybersecurity councils are common across the Baltic states. Generally, these function as informal or formal councils that convene representatives of military and civilian, private and public sector participants from critical sectors, and increasingly — critical functions that underpin the aforementioned. These councils collect holistic information on the state of cybersecurity across sectors, and are the only funnel of such information. (In the United States, the equivalent is the U.S. Department of Homeland Security’s Critical Infrastructure Partnership Advisory Council (CIPAC), which has authorities from 16 critical infrastructure sectors.) The findings of these cross-sectoral councils are increasingly critical to the development of transatlantic cybersecurity. A similar council should be established at the international level, between the United States and the EU, dedicating a channel to negotiate the security regimes of shared transatlantic critical functions, like ensuring the smooth operation of international finance or even maintaining internet infrastructure.
President Biden’s administration and EU leaders have both signaled commitments to renew the transatlantic partnership, especially in the digital arena, as highlighted by the recent formation of the U.S.-EU Trade and Technology Council. Of the 10 working groups within the council, four are working in the ambit of cybersecurity. These working groups should be used as a platform to advance cyber threat information sharing, providing a direct forum to channel the information from ENISA, NIST, and other national sectoral stakeholders. The aim of such a channel should be to triangulate the highest cybersecurity priorities, which should then branch off into more subsidiary cooperation channels with a feedback loop to higher, more senior executive levels.

U.S.-EU cybersecurity experience sharing is segmented between civilian and military sectors. However, the type of cyber threats both sectors share are increasingly similar and costly. The recent proposal to create an EU Joint Cyber Unit that will coordinate, share knowledge, and provide advanced warnings will draw together operational groups’ national cybersecurity authorities (CERTS), national defense authorities (military CERTs), and EU structures (ENISA and the Permanent Structured Cooperation; PESCO), among others. This Joint Cyber Unit can act as the mirror partner to the United States, which already has military and civilian sectors sharing risks via the Cyber Unified Coordination Group. The partnership between the United States and the EU in this capacity can take place via the U.S.-EU Trade and Technology Council, or a separate channel.
Endnotes


2 Alejandro Granja et al., “Recent Cyber Events: Considerations for Military and National Security Decision Makers.” NATO Cooperative Cyber Defence Centre of Excellence. 2021


4 Oliver Patel and Nathan Lea. “EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows.” SSRN. June 2020. https://iapp.org/resources/article/eu-u-s-privacy-shield-brexit-and-the-future-of-transatlantic-data-flows/. This environment has fostered the GAFAM firms to become data aggregators accounting for more than 55% of the used data capacity across the world. However, regulation of data in the US is light, and sector and state-specific, with examples like the California Consumer Privacy Act, or the NYDFS Cybersecurity Regulation.

5 The approach has been solidified by legislation like the General Data Protection Regulation (GDPR), which structures consent data relationships between data subjects, controllers, and handlers, or the eIDAS Regulation, which establishes harmonized digital identity documents across the EU.


8 The U.S. Committee on National Statistics echoed these findings in their 2017 consensus report.


Building Common Ground in Transatlantic Cybersecurity – A Baltic Approach


27 Ron Ross; Patrick Viscuso; Gary Guissanie; Kelley Dempsey; Mark Riddle, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.” National Institute of Standards and Technology. February 2020.


