Bendiek, Annegret; Kettemann, Matthias C.

Research Report

Revisiting the EU cybersecurity strategy: A call for EU cyber diplomacy

SWP Comment, No. 16/2021

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Bendiek, Annegret; Kettemann, Matthias C. (2021) : Revisiting the EU cybersecurity strategy: A call for EU cyber diplomacy, SWP Comment, No. 16/2021, Stiftung Wissenschaft und Politik (SWP), Berlin, https://doi.org/10.18449/2021C16

This Version is available at:
https://hdl.handle.net/10419/256677

SWP Comment
NO. 16 FEBRUARY 2021

Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy

Annegret Bendiek and Matthias C. Kettemann

In December 2020, the European Union (EU) presented its new strategy on cybersecurity with the aim of strengthening Europe's technological and digital sovereignty. The document lists reform projects that will link cybersecurity more closely with the EU's new rules on data, algorithms, markets, and Internet services. However, it clearly falls short of the development of a European cyber diplomacy that is committed to both "strategic openness" and the protection of the digital single market. In order to achieve this, EU cyber diplomacy should be made more coherent in its supranational, democratic, and economic/technological dimensions. Germany can make an important contribution to that by providing the necessary legal, technical, and financial resources for the European External Action Service (EEAS).

In 2019, the EU registered around 450 attacks on critical infrastructures in the energy and water supply sectors as well as information and communication technologies in the health, transport, and finance sectors. The vulnerabilities of technologically interdependent societies became particularly evident during the Covid-19 pandemic. In December, cybercriminals targeted the European Medicines Agency. In order to preserve its socio-political model, the EU must assert itself in a security environment that is characterized by mutual threat perceptions and an increasingly dynamic technological arms race. The director of the Technology and National Security Program at the Center for a New American Security, Paul Scharre, pointed out some time ago that the technology race is repeating the security dilemma of the nuclear age (*Foreign Affairs*, May/June 2019). How is the EU responding strategically to the changed global political environment? What role can the EU play in preventing cyberattacks, for example on power plants, in advance? Are there crises management structures in place at the European level to ensure immediate and comprehensive action if necessary?

EU Cybersecurity Strategy

Since 2015, the EU has been working on its response options to attacks from — and conflicts in — the cyber and information space (CIS). Some foreign and security policy initiatives have been launched in the last few years (see SWP Comment 19/2018).

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Worth mentioning here are, among others, the Diplomatic Response Framework (Cyber Diplomacy Toolbox) and the Cyber Defence Policy Framework (both 2018); the EU Cybersecurity Act and the EU toolbox for 5G security (both 2019); as well as the EU Security Union Strategy and the Screening of (Digital) Investment (2020). Since 2020, the EU has focused its activities — together with the member states — on building operational capacity to prevent, deter, and respond to serious cyber incidents in Europe. The current framework is set by the new EU Cybersecurity Strategy for the Digital Decade, presented in December 2020 by the European Commission and the High Representative for Foreign Affairs and Security Policy, Josep Borrell. It is closely linked to other Union initiatives, such as the Digital Single Market Strategy, the Commission's Economic Recovery Plan, and the Security Union Strategy 2020—2025.

The new cybersecurity strategy includes the establishment of a "Joint Cyber Unit" that will be tasked with strengthening the IT capabilities of defense communities in the field of cybersecurity and law enforcement agencies in cooperation with civilian and diplomatic communities. According to the strategy, the EU will also draw on the work of the European Defence Agency and promote cooperation in the military domain of operation, drawing on the newly created European Defence Fund. Furthermore, the EU will be given a "cybersecurity shield" to identify threats early and take countermeasures before damage is done. The Commission wants to establish an EU-wide "network of Security Operations Centres across the EU." It is to serve as a cooperation platform for the civilian and military authorities of the Union and member states that are responsible for cybersecurity and to improve coordination in the event of major attacks. To protect critical infrastructures, existing EU law and the 2016 EU Network and Information Security Directive (NIS Directive) are to be revised, and greater use will be made of artificial intelligence to identify cyberattacks against hospitals, utilities, and transport networks.

Since 2018, the EU has had the Cyber Diplomacy Toolbox at its disposal to counter serious cyberattacks (see SWP Comment 19/2018). It has thus designed its own sanctions regime against IT attacks that was deployed in July 2020 in the course of the technical and legal handling of the 2015 hacker attacks on the German parliament. To implement the cybersecurity strategy, proposals will be made under the Common Foreign and Security Policy (CFSP) to expand the EU Cyber Diplomacy Toolbox to effectively counter attacks on critical infrastructure, supply chains, and democratic institutions and processes.

Although the cybersecurity strategy refers to EU initiatives such as those to combat hybrid threats, the European Democracy Action Plan, as well as EU emergency and crisis management, the deepening of confidence- and security-building measures of EU cyber diplomacy toward third countries remains largely underexplored. The need for such actions has been noted, but no concrete examples or institutional venues to implement them have been provided. The cybersecurity strategy thus expresses a one-sided understanding of security policy that shows little awareness of the fact that technical and technocratic actions must be accompanied by diplomacy.

Desideratum Cyber Diplomacy

The one-sidedness of the EU cybersecurity strategy is a problem because international norm-building is a key element for trust and security in the cyber and information space. The EEAS needs to be empowered for this very task of cyber diplomacy by aligning its mandate accordingly. The current strategy neglects the important lesson of the nuclear age, namely that disarmament and trust-building actions lead to generally enhanced security. Political scientist Joseph S. Nye, for example, argues that, contrary to popular belief, deterrence in cyberspace can work. He is convinced that the development of international norms, which has so far been very limited, can have a positive

effect on security in the CIS. For this, he said, it is essential not to limit the principle of deterrence to classic territorial defense and immediate retaliation. Rather, cost-benefit analyses of unintended consequential costs would deter potential intruders from launching attacks.

The fact that a "cyberwar" has not yet taken place could be indicative of the effectiveness of this strategy. International norm processes can also dissuade state actors from attacking critical infrastructure. The norms for responsible state behavior in cyberspace, developed by the United Nations (UN) Group of Governmental Experts, prohibit attacks against critical infrastructure. The UN General Assembly negotiations demonstrate that, despite political differences, work is underway on common norms for lawful state behavior and due diligence in cyberspace. Under the Cyber Diplomacy Toolbox, the Horizontal Working Party on Cyber Issues is tasked with these matters; however, so far it has only had a coordinating and not a shaping role in EU cyber diplomacy due to lacking EU supranational competence.

Furthermore, there is still little consensus on standards for responding to cyber actions below the thresholds relevant under international law (retorsion); for the approval of hardware and software; for dealing with supply chain dependencies; and for vulnerability management. The November 19, 2020 "non-paper" by Germany and five other EU member states also remains unclear with regard to concrete actions. The dangers posed by proxies, i.e., non-state actors acting on behalf of the state, reduce the effectiveness of trust- and security-building actions. The Council of Europe's Budapest Convention is to be revised accordingly in order to take more effective action against non-state cybercrime with a second supplementary protocol. Another source of danger that should not be underestimated is the high number of low-threshold attacks, for example against small and medium-sized enterprises. It still needs to be clarified what counts as a critical IT security incident that must be reported, including to partner states outside Europe: Is it when the attackers penetrate the network and disrupt it, or already when they scan the infrastructure of a potential critical infrastructure facility and try to find weak points?

The cybersecurity strategy also mentions jointly coordinated NATO-EU situational awareness in the CIS, but it remains unspecific about its implementation. The potential of the Helsinki-based European Centre of Excellence for Countering Hybrid Threats to build "legal resilience" in relation to state interference is equally underutilized in EU-NATO cooperation. Some governments advocate active countermeasures, along the lines of the United States demonstrating its supremacy in cyberspace. Others, however, argue for the development of a consensual frame of reference that assigns accountability to states according to their resilience measures to prevent conflict escalation in the CIS. The EU strategy seeks to integrate both approaches more effectively than in the past. In order to realize this ambition, the EEAS must be given a stronger mandate in the future in terms of personnel, funding, and legal competence.

Digital sovereignty and resilience can only be achieved as a pan-European and pan-societal task that includes close coordination at the EU level as well as with democratic partners; moreover, economic policy and technological expertise must be explicitly included. This means that EU cyber diplomacy must set the framework for this, as the CIS is not bound by the competencies or borders of individual countries. Public institutions, business, the scientific community, and civil society must work hand in hand much more intensively at the European level than they have to date. The establishment of a European Cybersecurity Industrial, Technology and Research Competence Centre and a network of national coordination centres are a first good step. Cyber diplomacy can create the supranational, democratic, economic, and technological conditions, both internally and externally, to provide the necessary infrastructure, know-how, and cutting-edge technology.

The Supranational Dimension

Sectorally conceived policy silos — in which the digital dimensions of foreign, defense, and domestic policy are developed in parallel — are notoriously ill-suited to cybersecurity. On the other hand, it makes sense for the EU Commission to support the interlocking of internal market regulations, the fight against cybercrime, the CFSP, and the Common Security and Defence Policy, as well as initiatives of the Permanent Structured Cooperation. An annual implementation report, modeled after the progress reports on the implementation of the Security Union Strategy, would be beneficial and should give more attention to aspects that have been neglected so far, such as technical intelligence and information exchange.

In particular, it should systematically cover: the preparation and use of cyberattacks; the manipulation and sabotage of business, financial, and industrial markets; the increasing vulnerability of critical infrastructure; and the growing threat to the reliability of traditional defense systems from military hackers. Although the new Strategic Compass is intended to facilitate common EU situational awareness, this will require that internal and external cybersecurity agencies prepare to pool their intelligence in the EEAS when needed. Situational awareness should be underpinned by a "horizon scanning" facility, at least as a first step. Artificial intelligence should help establish early crisis detection.

This should be followed up by the development of an attribution procedure in the CFSP decision-making process. To date, there are no common standards for clearly identifying the perpetrator of a cyberattack. The Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities indicates that member states may use different methods and procedures for attributing malicious cyber activities, as well as employ "different methods and procedures to establish a degree of certainty on attributing a malicious cyber activity." However, the methods, procedures, definitions, and criteria of the member states are not to be harmonized, as attribution is to remain a sovereign act. The EEAS, with its Intelligence and Analysis Centre, would have to be provided new personnel and technical competencies if it is to (be able to) publicly state who is responsible for cyber incidents; this would be of particular importance for countering hybrid threats, which also include disinformation. Measures under the Cyber Diplomacy Toolbox do not require legally secured attribution in every case. Rather, they aim to defend against cyber incidents using political-communicative and technical means. It should be possible to tailor the use of resources, depending on the conflict situation.

In addition, it should be considered how the actions envisaged in the toolbox can be deployed in the event of a failure of key infrastructures in such a way that the ability to command, act, and function is maintained. Horizontal and vertical cybersecurity cooperation between the EEAS and the Commission on the one hand, and between the EU and the member states on the other, is key for the resilience of the ICT structures. This crisis management exists only as a blueprint and must be underpinned by the member states in terms of personnel, funding, and competencies.

The EU member states should recognize that digitalization challenges classic diplomacy at the national level, to the extent that the foreign policy role of the EU Commission changes in the course of implementing the European Digital Strategy: Its role is gaining more weight in cyber diplomacy. It is the Commission that urges member states to be vigilant about attempts to divide them, both externally and internally. This call for vigilance with regard to foreign direct investments or the acquisition of strategic assets, especially in the digital economy, by third countries could take even greater account of the risks posed by the volatility or undervaluation of European stock markets.

The Democratic Dimension

Digital foreign policy and cyber diplomacy must place more attention than traditional foreign and security policies to involving non-governmental interest groups and independent scientists in the policy process and to ensuring that the multistakeholder approach is applied as broadly as possible. To be sure, the practice of multistakeholder governance to date has been criticized for being misused by large digital corporations as an instrument for globalizing their own business interests and technical standards. However, the decisive integration of all societal stakeholders has ultimately proven to be a factor that safeguards fundamental rights. In particular, a reform of the global Internet governance infrastructure is as necessary as it is important, whereby the "democratic" dimension must be strengthened, for example by expanding the role of the Internet Governance Forum (IGF) as a global stakeholder meeting, consistently involving parliamentary representatives in IGF meetings, and including local and regional initiatives. Within this framework, the EU's external cyber foreign policy, mandated by the member states, will be able to continue to work toward ensuring that central institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) are geared toward inclusivity and participation of all social groups and not just toward the interests of business (see SWP Research Paper 14/2019). Parliamentary expertise is particularly in demand here, as it has been increasingly used in recent IGFs.

The technology-induced uncertainty in global politics is clearly reflected at all levels in a fundamentally changed perception of the opportunities and dangers of connectivity and interdependence. US political scientists Henry Farrell and Abraham L. Newman point out that interdependence is not only a promise but also a danger (*International Security*, July 2019). Global networks and supply chains in the financial and trading systems, in the management of the Internet, and in the global communications infrastructure, they argue, are highly asymmetric and can be used by powerful states as weapons against political opponents. The Corona pandemic and the assertive posturing of US and Chinese technology companies have given this impression more weight. On many issues — from access to the global financial and monetary system and innovative technology to needed medicines, digital communications, and network infrastructure — forums, podiums, and supply chains controlled by private actors constitute a source of power. States currently find themselves overwhelmed when their presidents can be stripped of their virtual megaphones by digital CEOs.

Against this backdrop, the revitalization of bilateral cyber diplomacy in the form of a trade and technology council between the EU and the United States has gained special attention for transatlantic cooperation since Joe Biden's election as US president. From the US perspective, any reconfiguration of a European cyber foreign and security policy should be based on an alliance of democratic multilateralists that must include the United States. Europe will only be strong enough to defend the functioning of the digital internal market based on European treaties against China and other authoritarian states if it cooperates with democracies such as Canada, Australia, Japan, the United States, and others, even if they only cooperate in the short term (ad hoc coalitions).

The literature already contains concrete proposals in this regard, some with far-reaching consequences. In October 2019, Richard A. Clarke and Rob Knake advocated the establishment of a US-led "Internet Freedom League" that would encompass all states committed to a free, open, and democratic Internet. It should form a digital block analogous to the European Schengen Area, within which data, services, and products could move freely, whereas all those states that do not respect freedom of expression and the protection of privacy and allow cybercrime would be excluded: "The goal should be a digital version of the Schengen

Agreement." In this cyber and information space, which according to the US view has yet to be developed, vulnerable online systems would be identified, their operators informed, and their resilience jointly worked on; malware and botnets would be eliminated at an early stage; and cyberattacks among the members would be prohibited — similar to the coordination of global health policy by the World Health Organization. Certainly, these goals are broadly consistent with, but go beyond, UN standards for responsible state behavior. Such a tech diplomacy alliance should integrate the EU's various cybersecurity programs in the Western Balkans and the six Eastern Partnership countries in the EU's immediate neighborhood, as well as in other countries worldwide.

The Economic-technological Dimension

In his influential study on the danger of fragmentation of the global Internet, political scientist Milton L. Mueller describes forcefully that all hopes for a global Internet depended directly on non-state and private actors continuing to play an essential role in its governance. There is no guarantee that individual European member states will not mimic the Internet censorship measures being pursued by Russia and China using deep packet inspection tools and banning VPNs unless they are countered by a strong social and legal corrective. This corrective can have both a cognitive and a power-political effect. In the European Commission, outstanding expertise has been built up in preparation of relevant legal acts on digital markets, services, algorithms, and data — in contrast to American, Chinese, and Russian standardization. This knowledge of regulations, standards, and norms is in high demand by various international players such as the African Union, the ASEAN states, Brazil, Australia, and South Korea.

Europe's role as an exporter of standards in data protection and data security, encryption, and cybersecurity also has economic consequences for players on the international market who want to continue to operate in the digital single market — despite the high requirements, for example, for compliance with standard contractual clauses for data transfers, which were made even more stringent by the restrictive case law of the European Court of Justice in July 2020. The EU's cyber diplomacy must negotiate the future global standard contractual clauses on data transfer as well as a new transatlantic Privacy Shield with the United States in the Transatlantic Council on Trade and Technology.

EU approaches to the management of critical Internet resources also imposed by the Digital Services Act and Digital Markets Act will in the future envisage even stricter targets than before: Dependencies on individual suppliers are to be diversified. Auditing by means of an EU-wide IT security label is to link market access for all market participants to minimum standards and certifications. Encryption technologies are to ensure high European security standards in the future in order to guarantee the integrity and security of data. However, civil society and the business community are critical of mandatory decryption or master keys for law enforcement agencies, as demanded by individual governments.

An important initiative for securing European digital sovereignty is the strengthening of the European cloud and data infrastructure project GAIA-X. In order to assert themselves against non-European market power, leading member states and the European Commission are attempting to bundle European companies and leverage their own values based on the EU treaties as a competitive advantage against third parties. Data protection and data security should no longer be seen as a hindrance to technological development, but as a driver of innovation — especially in light of the fact that quantum computing can already circumvent common methods of cryptography.

EU digital sovereignty is complex, but that does not mean that everything should now be done autonomously via the EU

Commission, but rather that a technically sophisticated strategic choice should be made to control those truly critical components. Cyber diplomacy of the EEAS, in close consultation with the European Commission, requires an intensive cooperation between public and private partnerships if it is to be technically competitive. Therefore, it should strive to promote the development of trusted IT through these partnerships. Artificial intelligence can be used associatively for the early detection of attacks on automated systems. Finally, information about Indicators of Compromise, i.e., characteristics and data that indicate a system or network is compromised, must be made available to all stakeholders so that everyone can participate in the solutions offered.

The cyber diplomacy conducted by EEAS, in cooperation with the Commission or the Cyber Security Agency, should be enabled to raise these technological requirements to the level of European infrastructures so that industry and the owner of the critical infrastructures can benefit from the results. Last but not least, the Commission intends to broaden the scope of what critical infrastructure should include. In addition to traditional sectors such as energy, institutions of national and strategic interest will also be targeted. In the future, the Commission will have an even greater role in ensuring the availability, integrity, and confidentiality of European data through a single market external policy.

Update of Cyber Diplomacy Needed

A world that is growing together needs common rules and a binding legal framework so that common markets can develop and the security dilemma can be resolved. If EU member states turn to a truly EU cyber diplomacy that is guided by the maxim of "strategic openness" in its institutional, democratic, and economic dimensions, they can ensure that the post-war era will only not become the digital pre-war era. Strategic openness is central to maintaining the internal market in order to effectively counter the siren songs of mercantilist isolationism and territorial sovereignty thinking, even in the digital age. The EU's digital self-assertiveness manifests in reducing dependencies, promoting the empowerment of civil rights, holding platforms accountable, and increasing the competitiveness of the European economy.

With this aspiration in mind, EU cyber diplomacy should, *first*, help citizens retain informational self-determination over their personal data. *Second*, cyber diplomacy, in the service of the EU's digital sovereignty, is linked to the strategic capacity to act and presupposes that the Union can also assert its ideas on data protection and security internationally. *Third*, a European "resovereignization" in cyber diplomacy in the digital age means realizing that a minimum degree of dominance or control by the EU over the necessary technological resources — from Internet nodes to cloud infrastructure to international standard-setting — is what makes digital sovereignty possible in the first place. *Fourth*, this includes ensuring that European laws are applied to cyberspace and are enforced by European courts. China and the United States, for example, essentially limit themselves to domestic providers for critical infrastructure (hardware and software) for cybersecurity reasons. *Fifth*, in the spirit of reciprocity and competitiveness, harmonization of IT security legislation and procurement and licensing rules at the EU level would be logical. Cooperation between the EU and democracies such as the United States, Canada, Singapore, South Korea, and Taiwan could promote this.

These goals are served by the EU's new and planned legal acts and strategies on data, markets, services, and algorithms in Europe and, most recently, on cybersecurity. As the Union moves forward in this way, member states should also be prepared to update Europe's narrative as a force for peace in the digital age through more robust and coordinated foreign, security, and defense policies and by honoring their

strategic orientation and institutional anchoring in EU cyber diplomacy. This would at least be the logical consequence. Qualified majority decisions are certainly needed to be able to respond with restrictive measures in the event of serious cyberattacks.

But harmonization is not always the path to optimization. A pan-European and pan-societal approach to cybersecurity means formalizing the exchange of knowledge between institutions, security authorities, academia, and industry. Defense and diplomacy in the cyber and information space remain sovereign tasks. At least since the ruling of the Federal Constitutional Court (BVerfG) on the Federal Intelligence Service of May 19, 2020, and the BVerfG's non-acceptance decision of December 16, 2020, it has become clear that the obligations of all German authorities under the rule of law do not end at the state's external borders, and that the state is fundamentally liable for violations of fundamental rights abroad — this also applies in the CIS. This means that close cooperation is required in this complex cybersecurity architecture. At the same time, it places new demands on constitutional principles in Germany, such as the separation between defense and police powers and the limits to the deployment of the military within German borders. Effective and accountable cybersecurity policy at the national level creates conditions that enable administrative assistance at the EU level and in cooperation with alliance partners in a legally secure manner — with EU cyber diplomacy as the centerpiece.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1861-1761
ISSN (Online) 2747-5107
doi: 10.18449/2021C16

(English version of SWP-Aktuell 12/2021)

Dr. Annegret Bendiek is Deputy Head of the EU/Europe Research Division at SWP.
PD Dr. Matthias C. Kettemann, LL.M. (Harvard), is Research Programme Head at the Leibniz Institute for Media Research/Hans-Bredow-Institut and Research Group Leader at the Humboldt Institute for Internet and Society and at the Sustainable Computing Lab at the Vienna University of Economics and Business.