Comparative Analysis on Cyber Diplomacy in EU and US

Carmen-Elena CÎRNU[1], Carmen-Ionela ROTUNĂ[1], Ioana-Cristina VASILOIU[1,2]
[1]National Institute for Research and Development in Informatics - ICI Bucharest
carmen.cirnu@ici.ro, carmen.rotuna@ici.ro, ioana.vasiloiu@ici.ro

[2]Bucharest University of Economic Studies
ioana.vasiloiu@csie.ase.ro

Abstract: Globally, there is a continuous increase in the number of cyberattacks by independent hackers and non-state actors. The European Union and the United States of America have recognized the importance of cyber security and cyber diplomacy for government institutions, companies and individuals. Coherence and synchronization between global cyber initiatives are needed to effectively increase cyber resilience and deter cyberattacks. The current paper conducts a comparative analysis of cyber diplomacy in the EU and the US with the aim of highlighting the best policies, diplomatic measures, frameworks and practices for increasing cyber resilience. It also identifies the institutions responsible in the EU vs. the US, compares the EU Cyber Diplomacy Toolbox and the US Cyber Diplomacy Act and identifies and compares preventive measures, cooperative measures, stability measures, restrictive measures and supportive measures. The aim is to outline the most fruitful and effective measures and to support homogenization at a global level.
Keywords: Cyber diplomacy, treaties, war, cybersecurity, hackers, state actors.

INTRODUCTION

Cyber diplomacy addresses the joint efforts of governmental actors entities to develop a series of norms and rules that regulate the behaviour of state and private actors in cyberspace. The goal is to prevent and sanction cyberattacks and to achieve a reliable, stable resilient and secure cyberspace. Cyber diplomacy treaties are elaborated under the auspices of international law (Delmeire & Lavadoux, 2021), in line with the national laws and address both state and non-state actors.

In Europe, the term is used concerning a series of strategies and initiatives that the EU implements to encourage cyber security/ responsible behaviour in cyberspace. On the one hand, there are internal strategies, which focus on the effects of attacks on the member states, and on the other hand, there are external strategies that have as their objective the relationship with global cyberspace.

During the pandemic period, cybercrime increased in proportion and this phenomenon was supported by the increased use of remote working systems as most companies had to

https://doi.org/10.54851/v5i1y202307

minimize human interaction to prevent the spreading of the virus. There were various cyberattacks in all domains of activity. Several high-impact attacks targeted medical facilities and pharmaceutical companies.

Cyberattacks on health care systems have risen significantly since the pandemic began last year. One trend is criminals taking over servers, stealing personal data, and then charging money to allow officials to get back in and threatening to sell the data online — a type of attack known as ransomware. Group-IB, a cybersecurity firm, said ransomware grew by 150 percent in 2020 (Group-IB, 2021).

In October 2020, a hacker gain access to Finnish patients' data and used it to blackmail them. In France, two hospitals were victims of cyberattacks in one week in February 2021 (France24, 2021). Similarly, many hospitals in the US were attacked last year and the alleged perpetrator was a group of Russian cyber attackers (Haeck, 2021). Also, the most significant cybercrime on the health system took place in Ireland which affected the majority of health services, including COVID-19 institutions, cancer treatment facilities, and maternity hospitals.

Not only the medical domain was severely affected by cybercrime. In Germany was detected a cyberattack targeting the email accounts of the members of the federal parliament. It affected seven members of the Bundestag and 31 members of parliament and it was unclear whether data leak occurred (Reuters, 2021).

The major causes of all these attacks are the use of legacy systems and the insufficient cyber-training of employees. In some cases there is a lack of budget, thus the old machines are not replaced by new ones.

The EU, along with its Member States, have noticed the significance of the continuous EU cyber diplomacy engagement. At the same time, there is a necessity for coherence among the EU cyber initiatives to enhance cyber resilience effectively. Therefore, the Member States are encouraged to further intensify their efforts on cyber dialogues within the framework of effective policy coordination and emphasize the importance of cyber capacity building in third countries. The major concern of the European Union is the continuously increasing capacity of state and private actors to pursue their goals by launching malicious cyber activities varying in sophistication, goal, intensity, duration, complexity, amplitude, and impact. (EU Council, 2017).

CYBER DIPLOMACY - STATE OF THE ART WORLDWIDE (POLICIES, DIPLOMATIC MEASURES)

Back in the day, when there was no cyberspace, diplomacy was used to adjust incompatible interests by negotiation and concession (Wight, 1979). However, today, in an era of cyberspace, which is constantly developing, there emerges a need for cyber instruments to enable more effective implementation of diplomatic strategies. At the same time, this need has generated a spectrum of government-led efforts that can benefit from the diplomat's methods and mentality. The government-led actions refer to cyber diplomacy policies, diplomatic resources, and functions used to secure national interests concerning cyberspace.

According to Attafa et al. 2020), due to globalization, the cyber diplomacy need to be occurred in 2007, simultaneously with the cyber-attack on Estonia, consisting of crippled computer networks which impacted both government and corporate sites. At that point, there was no international political mechanism for raising the importance of the aggression, pleading for support from other countries, or condemning the aggressors. Since then, these attacks have generated the need for governments to start thinking about cyber strategies to protect their national interests.

Cyber security has become an essential aspect of everyday life, which, as reported by Buchan (2016), requires norms and regulations for both state and non-state actors in cyberspace.

These norms refer to a secure, open, stable and free cyberspace and are promoted and applied via multilateral agreements. They are used to prevent cyberattacks and promote cyber security at both internal and international levels.

In Barrinha's opinion (2017), cyber diplomacy can be portrayed as diplomacy in the cyber environment or as the usage of diplomatic resources and the enactment of diplomatic procedures to ensure national interests concerning cyberspace. Such interests are commonly specified in national cyberspace or cybersecurity strategies, frequently referencing the diplomatic agenda. General topics on the cyber-diplomacy agenda incorporate internet freedom, cybersecurity, internet governance, and cybercrime.

Barrinha et al. (2017) state that cyber diplomacy is executed fully or partially by diplomats, meeting in bilateral formats (for example, the EU–US Cyber Dialogue) or multilateral fora (for example, the UN). Moreover, diplomats interact with non-state players, such as leaders of internet enterprises (Google, Facebook) or civil society communities.

In this regard, Estonia has adopted a two-direction approach to cyber diplomacy, starting by developing a framework regarding cyber stability (developing a cyber stability framework in international organizations, improving expertise, staying on top of the development of new technologies) and using deterrence to prevent threats to the country's security (partnerships, attribution, response measures, capacity building). At the same time, the policies concerning cyber diplomacy intend to improve cyber resilience and increase collaboration with other state actors aligned with the foreign policy demands. Moreover, the country has adopted the Foreign Policy Strategy 2030, which aims to advocate for international cyber policy, develop global cybersecurity initiatives and boost bilateral cooperation based on democratic principles and human rights.

CYBER DIPLOMACY - STATE OF THE ART WORLDWIDE (POLICIES, DIPLOMATIC MEASURES)

The beginning of cyber diplomacy in the EU and the US

Following the 2007 attacks on Estonia's infrastructure, the European Union has been forced to amplify its strategy for cyber security. In the meantime, an increasing number of cyberattacks in the EU have extended awareness of risks and threats connected to cyberspace. Therefore, the development of an exhaustive legal, policy and institutional framework covering all key policy areas of the EU, including cybercrime and cyber defense, appeared. (Cîrnu, 2017; Painter C, 2022).

It started with creating new institutions based on new legal measures, the European Network and Information Security Agency (ENISA - 2004) and the European Cybercrime Center - Europol (EC3 - 2013) being two examples. The EU has constructed an elaborate cybersecurity ecosystem. A multi-level (national, regional and global) system of cybersecurity governance across three distinct policy areas has emerged. (ENISA, 2020).

For the European Union, the phrase 'cyber diplomacy' is not exclusively about the EU's steps toward establishing legally enforceable, multilateral accords for trustworthy conduct in cyberspace. Instead, the term is utilized for a spectrum of strategies and initiatives the that the EU implements to encourage cybersecurity. There are two axes covering the European Union's approach to cyber diplomacy: international (centered on developing multilateral and global strategies) and internal cybersecurity (focused on the consequences of cyberattacks on the EU's internal security). (EU Digital Diplomacy 2022)

The desired EU option for cyber warfare in the cyber domain is diplomacy and cooperation. The 2016 EU Global Strategy (EUGS) is proof, defining the aims and requirements of cyber diplomacy. The Strategy pursues to support, agreements on responsible state behaviour in

cyberspace based on existing international law,' ,multilateral digital governance, and a global cooperation framework on cybersecurity', based on partnerships between like-minded nations, associations, civil society, the private sector, and specialists.

Cyber diplomacy's pillars are cyber capacity and confidence-building with counterparts. The main elements of these pillars, according to European Commission, can be outlined as follows:

- developing and building the resilience of organizations able to react to and recover from cyber threats;
- securing diplomatic obligations to maintain an open, free and safe cyberspace;
- encouraging inclusive growth and the sustainable evolution of digital infrastructure;
- enhancing digital markets and ensuring a secure online economy;
- developing cyber defence techniques to defend military networks, assets, and defence institutions.

In the U.S., there have been different initiatives and policies in the field of cybersecurity, such as the 2002 National Strategy to Secure Cyberspace, the 2006 National Infrastructure Protection Plan, and the 2007 National Strategy for Information Sharing. In January 2008, was prepared the Comprehensive National Cybersecurity Initiative to make the United States more secure against cyber threats. The directives establishing this initiative are classified. The appointment of a cybersecurity coordinator and advisor in late 2009 shows the U.S.' commitment to taking the cybersecurity issue seriously. The job involved securing critical infrastructures and government networks by coordinating the federal government's cybersecurity initiatives. The position also included ensuring that agencies have money allocated for cybersecurity priorities and harmonising the government's response to a significant cyber incident.

Moreover, in 2021, the US House passed the Cyber Diplomacy Act. This bill aimed to facilitate American global leadership on cyber security and support cyber diplomacy-related issues on the international scene. It was also a matter of enhancing the federal government's ability to react to cyberattacks (see Figure 1).

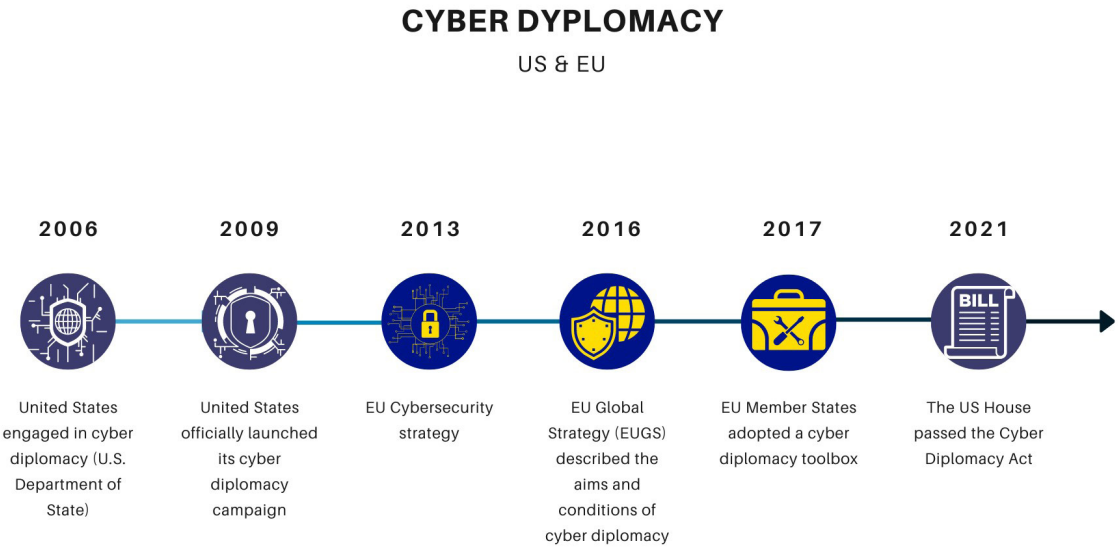

Figure 1. *Cyber Diplomacy US & EU (Source: own)*

The responsible institutions in EU vs. US

Being two different structures considering their history and organisation's manner, the E.U. and the U.S. have various institutions and systems in place to manage cyber security and cyber security within their borders.

Figure 2 below shows the institutions responsible for these issues in both entities.

With its elaborate internal structures, the EU is actively shaping the legal and policy framework of international cybersecurity, being an actor and part of the institutional framework at the international level.

In the EU, actions linked to cyber diplomacy mainly involve the Common Foreign and Security Policy (CFSP) and its principal component - the Common Security and Defence Policy (CSDP). The CSDP allows the EU to lead in peace-keeping actions, dispute prevention, and enhancing global security. It is essential to the EU's thorough approach to crisis management, drawing on civilian and military assets. For the Member States and the EU organisations, the cyber security and cyber diplomacy matters are addressed by the 2013 EU Cyber Security Strategy, the 2014 EU Cyber Defence Policy Framework (CDP), the 2016 NIS (Network and Information Security) Directive, the 2016 Global Strategy for the European Union's Foreign and Security Policy, and the actions of ENISA (the European Network and Information Security Agency, EC 3 (the European CyberCrime Centre) at Europol and CERT-EU.

These measures belong to the CFSP and are

EU	US
The European External Action Service (EEAS)	The Department of State
Single Intelligence Analysis Capacity (SIAC)	The Bureau of International Cyberspace Policy
The EU Intelligence and Situation Centre (EU INTCEN)	International Cyberspace Security (ICS)
The EU Hybrid Fusion Cell	International Information and Communications Policy (ICP)
EU Intelligence Division/EUMS INT	Digital Freedom (DFU)

Figure 2. *Cyber Diplomacy Institutions*

described under the appropriate requirements of the Treaties. They are proposed as alternatives for deliberation, where applicable, and do not prevent action by any individual Member State or action harmonised between the Member States.

This Framework's measures are classed into five categories:

- Preventive actions;
- Cooperative measures;
- Stability initiatives;
- Restrictive measures;
- Possible EU support to Member States' lawful responses.

INTCEN (the EU Intelligence and Situation Centre), in collaboration with the CSIRTs network lead by the alternate Presidency, the EC3, ENISA, or CERT-EU, will adopt a leading position in aggregating all-source information and organizing an analysis and political assessment of a single, or across events.

At the same time, in the U.S., the Bureau of Cyberspace and Digital Policy coordinates the U. S. Department's cyberspace and digital diplomacy work. It seeks to facilitate reliable state behaviour in cyberspace and advance procedures that protect the integrity and security of the Internet's infrastructure, serve U.S. interests, encourage competitiveness, and support democratic values. The Bureau manages the national security challenges, economic possibilities, and values concerns raised by cyberspace, technologies, and digital policy and promotes measures and standards that are equitable, transparent, and support U.S. values.

The Bureau has three policy units: International Cyberspace Security (ICS), International Information and Communications Policy (ICP), and Digital Freedom (DFU):

- ICS fosters cyberspace stability and security, protecting U.S. national security interests in cyberspace. It conducts diplomatic engagement on global cyberspace security in multilateral, regional, and bilateral forums and works with like-minded states to execute coordinated responses to malicious cyber activity.
- ICP cultivates an interconnected, visionary, and safe digital economy that reflects the U.S.' joint interests. It encourages competitive and secure networks, including 5G, and protects telecom services. ICP associates with U.S. companies, civil society, and foreign governments and promotes U.S. leadership on digital issues in multilateral institutions to attain these objectives.
- DFU has its activity regarding privacy, security, content moderation procedure, tech platform regulation, human rights, and civic engagement. Its work refers to defending against actions to legitimize and assume repressive and rigid practices in cyberspace.

EU CYBER DIPLOMACY TOOLBOX VS. CYBER DIPLOMACY ACT

To comprehend the differences and similarities between the EU Cyber Diplomacy Toolbox and the US Cyber Diplomacy Act, the measures covered within every cyber security policy were listed, as Table 1 shows. (CCDCOE, 2020; Schaffer, 2022)

First, the EU Cyber Diplomacy Toolbox is referred to as a „framework on a joint EU diplomatic response to malicious cyber activities." In contrast, the US Cyber Diplomacy Act is „an act to support United States international cyber diplomacy." (Bendiek, 2020)

Both frameworks contain preventive, cooperative, and stability measures, even if their definitions are slightly different. The most significant distinction is that the EU states the restrictive measures within their EU Common Foreign and Security Policy framework. These can include, among other things, „travel bans, arms embargoes, freezing funds or economic resources." (Kerry, 2017)

Table 1. *EU Cyber Diplomacy Toolbox vs US Cyber Diplomacy Act*

EU Cyber Diplomacy Toolbox (EU Council, 2017)	**US Cyber Diplomacy Act (117th Congress, 2021)**
Preventive measures: EU-supported Confidence Building Measure, awareness raising on EU policies, EU cyber capacity building in third countries.	Reducing and limiting the risk of escalation and retaliation in cyberspace, damage to critical infrastructure, and other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public.
Cooperative measures: Cooperation through EU-led political and thematic dialogues or démarches by the EU Delegations.	Cooperating with like-minded democratic countries that share common values and cyberspace policies with the United States, including respect for human rights, democracy, and the rule of law, to advance such values and policies internationally.
Stability measures: Statements by the High Representative and on behalf of the Council of the EU, EU Council conclusions, Diplomatic démarches by the EU delegations, Signalling through EU-led political and thematic dialogues.	Securing and implementing commitments on responsible country behaviour in cyberspace based upon accepted norms.
EU restrictive measures (sanctions).	Encouraging the responsible development of new, innovative technologies and ICT products that strengthen a secure Internet architecture that is accessible to all.
Norms of responsible behaviour: The EU claimed the need for voluntary, non-binding norms. The UN GGE norms are endorsed and progress should be made on their implementation. (EU Cyber Direct, 2022).	Norms of responsible behaviour: As stated in the 2018 National Security Strategy, the US non-binding norms of state behaviour during peace are an essential components in a cyber resilient framework. The US attended all meetings of the UN Group of Governmental Experts (UNGGE) as well as the latest Open-Ended Working Group. (EU Cyber Direct, 2022).
Possible EU support to Member States' lawful responses	Clarifying the applicability of international laws and norms to the use of ICT.
	Advancing, encouraging, and supporting the development and adoption of internationally recognized technical standards and best practices.

BEST PRACTICES & DIRECTIONS IN CYBERSECURITY

The cyber diplomacy treaties between countries that apply severe sanctions might significantly reduce the number of attacks by discouraging cyber crimes. This would presume that each country deals internally with extremist cyber organizations by applying drastic measures that sanction these types of actions. There are several measures that can be taken, one of them being financial sanctions proportional to the severity of the attack and the impact. For example, a minor event leading to the unavailability of non-essential services for a few minutes with minor financial and image impact could be categorized as a minor event and minor financial sanctions could be applied. At the other extreme, a major cyber attack that results in the non-functioning of essential services and causes loss of human life could be sanctioned with imprisonment and the payment of considerable damages to the victim's families and the affected essential service provider. This is at the internal country level. A question arises in the case when an actor from state A carries out a massive attack on an essential services operator from another state and there is a cyber diplomacy treaty between the 2 states. In this case, there are 2 options: the actor is judged either according to the laws of his country or according to the laws of the country where he carried out the malicious actions. These aspects can be regulated in cyber diplomacy treaties between states.

Another aspect that must be integrated into the cyber diplomacy treaties is the case where the origin of the attack and the identity of the attackers are unknown.

At this point in time if an international cyberattack is carried out there are no consequences for the country of origin of the attacker. State actors may be reluctant to sign a diplomacy treaty that holds them accountable to some degree for the actions of their citizens.

As expressed in the EU cyber diplomacy toolbox, the European Union has an invested interest in establishing criteria and norms for cyberspace security. The EU's safety, stability, and foreign influence on global security are implicated. Thus, EU diplomatic missions should tactically deploy an ambitious, coordinated, coherent action in cybersecurity. This effort should concentrate on these three major domains:

- Continue developing and deploying its cyber diplomacy toolbox, which is still in its beginnings. A priority should be the development of actions that improve the accountability of individuals and entities liable for malicious attacks against the EU.
- Invest in creating a leading position in shaping global standards for responsible state conduct in cyberspace. A critical part of the EU's diplomatic missions in partner nations should be the diligent promotion of international criteria for an open, free, secure cyberspace.
- Strengthen member states' collaboration in the prevention and management of cyberattacks.

CONCLUSION

In conclusion, cyber diplomacy refers to efforts made by state representatives to shape the governance of cyberspace at the international level to discourage or penalize cyberattacks. Wordwide in recent years, specifically during the COVID pandemic the number of cyberattacks carried out by state and non-state actors has increased. This phenomenon amplified mainly because many public or private organisations had to set up remote working environments for their employees. The insufficient cyber education and legacy systems created black spots for cybercriminal to attack critical infrastructure facilities such as hospitals, financial and energy essential services operators.

The need for diplomacy in the cyber era is unquestionable, yet developing and applying it is new. Cyber diplomacy emerged based on the expansion of the governing systems of cyberspace recently. It deals with issues arising in cyberspace, from internet governance

to cybercrime, cyber espionage to critical infrastructure protection, and responsible state behaviour in cyberspace. Initially, cyber issues were treated as technical problems; afterward - as external elements of domestic policies. And now, they are acknowledged as an important foreign policy matter.

The European Union and the USA have recognized the importance of cyber security and cyber diplomacy for government institutions, companies and individuals. Coherence and synchronization between global cyber initiatives are needed to effectively increase cyber resilience and deter cyberattacks.

This research paper carries out a comparative analysis of cyber diplomacy actions in the EU and the US with the purpose to identify diplomatic measures, policies, frameworks and practices for increasing cyber resilience. It also identifies the institutions responsible in the EU vs. the US, compares the EU Cyber Diplomacy Toolbox and the US Cyber Diplomacy Act and identifies and compares preventive measures, cooperative measures, stability measures, restrictive measures and supportive measures. The results of the study are effective measures that can be used to support homogenization at a global level.

REFERENCE LIST

117th Congress (2021) *H.R.1251: Cyber Diplomacy Act of 2021*. https://www.congress.gov/bill/117th-congress/house-bill/1251/text [Accessed 12 December 2022].

Attatfa A., Renaud K. & De Paoli S. (2020) Cyber Diplomacy: A Systematic Literature Review, *Procedia Computer Science*. 176, 60-69. doi: 10.1016/j.procs.2020.08.007 [Accessed 15 November 2022].

Barrinha, A. & Renard, T. (2017) Cyber-diplomacy: the making of an International Society in the digital age. *Global Affairs*. 3, 353–364. https://www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924 [Accessed 12 November 2022].

Bendiek A. (2018) The European Union's Foreign Policy Toolbox in International Cyber Diplomacy, *Cyber, Intelligence, and Security*. 2 (3), December 2018. https://www.inss.org.il/wp-content/uploads/2019/01/Bendiek.pdf [Accessed 12 November 2022]

Buchan, R.J. (2016) Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm, *Journal of Conflict & Security Law* 21 (3), 429-453. doi: 10.1093/jcsl/krw011 [Accessed 16 November 2022].

CCDCOE. (2020) *Si vis cyber pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action*. https://ccdcoe.org/incyder-articles/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/ [Accessed 10 January 2023].

Cîrnu, C.E., (2017) Cyber Diplomacy – Addressing the Gap in Strategic Cyber Policy. *The Market for Ideas*. 7-8. https://www.themarketforideas.com/cyber-diplomacy-addressing-the-gap-in-strategic-cyber-policy-a388/ [Accessed 24 November 2022].

Council of the European Union (2017) *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*. https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf [Accessed 11th November 2022]

Delmeire, M. & Lavadoux F. (2021) *EU Cyber Diplomacy*. https://www.eipa.eu/blog/eu-cyber-diplomacy-101/ [Accessed 16 November 2022].

ENISA. (2020) *External Action Service Framework for a joint EU diplomatic response to malicious cyber activities "cyber diplomacy toolbox".* https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-eeas-eu-cyber-diplomacy-toolbox.pdf [Accessed 21 November 2022].

EU Council. (2017) *Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf [Accessed 18 November 2022].

EU Cyber Direct. (2022) *Compare European Union and United States*, Retrieved from Horizon website: https://eucyberdirect.eu/atlas/country/european-union/compare/united-states [Accessed 11 November 2022].

EU Digital Diplomacy. (2022) *Council Conclusions, Foreign Affairs Council.* https://via.diplomacy.edu/https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf#annotations:V7RrZhLVEe2UOOONlOVDAQ [Accessed 23 November 2022].

France24. (2021) *Cyber attacks hit two French hospitals in one week*. https://www.france24.com/en/europe/20210216-cyber-attacks-hit-two-french-hospitals-in-one-week [Accessed 11 December 2022].

Group-IB. (2021) *Ransomware empire prospers in pandemic-hit world. Attacks grow by 150%* (n.d.). https://www.group-ib.com/media-center/press-releases/ransomware-2021/ [Accessed 16 December 2022].

Haeck, P. (2021) *Irish hospital hack exposes EU cyberattack vulnerability.* Politico. https://www.politico.eu/article/irish-hospital-hack-highlights-eus-weak-spots/ [Accessed 6 November 2022].

Kerry, C. (2017) *The Cyber Diplomacy Act of 2017: Giving Cyber the Importance It Needs at the State Department.* https://www.lawfareblog.com/cyber-diplomacy-act-2017-giving-cyber-importance-it-needs-state-department [Accessed 11 November 2022].

Painter, C. (2022) *Diplomacy in Cyberspace.* https://afsa.org/diplomacy-cyberspace [Accessed 2 November 2022].

Reuters. (2021) *Russian hackers target German parliament again.* https://www.reuters.com/article/uk-germany-politics-cyber-idAFKBN2BI25P [Accessed 2 December 2022].

Schaffer, A. (2022) *It's a big day at the State Department for U.S. cyberdiplomacy.* https://www.washingtonpost.com/politics/2022/04/04/its-big-day-state-department-us-cyberdiplomacy/ [Accessed 6 December 2022].

Wight, M. (1979) *Systems of states.* Leicester. Leicester University Press.