Revista CIDOB d'Afers Internacionals
ISSN: 1133-6595
ISSN: 2013-035X
publicaciones@cidob.org
Barcelona Centre for International Affairs
España

Munkøe, Malthe; Mölder, Holger
Cybersecurity in the era of hypercompetitiveness: can the EU meet the new challenges?
Revista CIDOB d'Afers Internacionals, núm. 131, 2022, Mayo-Septiembre, pp. 69-92
Barcelona Centre for International Affairs
España

DOI: https://doi.org/10.24241/rcai.2022.131.2.69/en

Revista CIDOB d'Afers Internacionals
n.º 131, p. 69-92
ISSN:1133-6595 I E-ISSN:2013-035X
DOI:doi.org/10.24241/rcai.2022.131.2.69/en

Reception date: 25.11.21
Acceptance date: 20.04.22

# Cybersecurity in the era of hypercompetitiveness: can the EU meet the new challenges?

## La ciberseguridad en la era de hipercompetitividad: ¿puede la UE afrontar los nuevos retos?

**Malthe Munkøe**
Senior Advisor, BusinessEurope (writing in his private capacity). *malthemunkoe@gmail.com.*

**Holger Mölder**
Associate Professor in International Relations, TalTech-Tallinn University of Technology.
*holger.molder@taltech.ee. ORCID: https://orcid.org/0000-0003-2481-2735*

***How to cite this article:*** Munkøe, Malthe and Mölder, Holger. "Cybersecurity in the era of hypercompetitiveness: can the EU meet the new challenges?". *Revista CIDOB d'Afers Internacionals*, issue 131 (September 2022), p. 69-92. DOI: doi.org/10.24241/rcai.2022.131.2.69/en

**Abstract**: In her 2021 State of the Union address, European Commission President Ursula von der Leyen stressed the need to improve EU cybersecurity. The threat landscape is diverse and changing, and includes disinformation and fake news, cyber-attacks on government infrastructure and interference in elections in third countries. With this in mind, in December 2020 the EU unveiled a new Cybersecurity Strategy that includes legislative and institutional initiatives: from the revision of the NIS Directive – the EU's first cybersecurity legislation – to the establishment of a cybershield to identify large-scale cyber-attacks. To be effective in this field, which involves a multitude of actors, the EU will need to ensure robust cooperation and information exchange, both at national and European level, as well as with NATO.

**Key words**: European Union, cybersecurity, hypercompetitiveness, European integration, information warfare, economic security

***Resumen****: En su discurso de 2021 sobre el estado de la Unión, la presidenta de la Comisión Europea, Ursula von der Leyen, recalcó la necesidad de mejorar la ciberseguridad de la UE. El panorama de las amenazas es diverso y cambiante: desinformación y noticias falsas, ataques informáticos contra infraestructuras gubernamentales, injerencia en elecciones de terceros países, etc. Ante ello, en diciembre de 2020, la UE dio a conocer una nueva Estrategia de Ciberseguridad que incluye iniciativas legislativas e institucionales: desde la revisión de la Directiva NIS –la primera legislación sobre ciberseguridad de la UE– hasta el establecimiento de un ciberescudo para identificar los ataques cibernéticos a gran escala. Para ser efectiva en este campo, en que participan una multitud de actores, la UE deberá garantizar la cooperación y el intercambio de información de forma sólida, tanto a escala nacional como europea, así como con la OTAN.*

***Palabras clave****: Unión Europea, ciberseguridad, hipercompetitividad, integración europea, guerra informativa, seguridad económica*

Cybersecurity has recently moved from relative obscurity to a topic of high political importance. In 2021, the European Commission President Ursula von der Leyen highlighted the issue in her annual State of the Union speech given on September 15. She devoted a considerable amount of time to this particular subject, noting that: "We cannot talk about defence without talking about cyber. If everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces. And we should not just be satisfied to address the cyber threat, but also strive to become a leader in cyber security" (von der Leyen, 2021).

With cyber entering the top of the EU policy discourse it is no surprise that a number of initiatives are set to be rolled out and developed, both through new legislation pertaining to the cyber domain and new institutional developments. In her speech von der Leyen even went as far as to call for a "European Cyber Defence Policy", heralding the centrality awarded to cybersecurity in EU policymaking.

**The cybersecurity threat against Europe is multifaceted in its nature, stemming from criminal groups, groups with some alleged affiliation to geopolitical rivals, and regular cybersecurity forces deployed as part of the military apparatus other states can unleash in the event of conflict.**

The cybersecurity threat against Europe is multifaceted in its nature, stemming from criminal groups, groups with some alleged affiliation to geopolitical rivals, and regular cybersecurity forces deployed as part of the military apparatus other states can unleash in the event of conflict, as demonstrated by the ongoing Russian-Ukrainian war. Similarly, the nature of the cyber threats varies from operations seeking to degrade or interrupt infrastructure to cyber espionage, and from extortive schemes including identity fraud to procuring compromising information e.g. for blackmail purposes. This diversity of threats arising from the cyber domain necessitates a multipronged approach, as well as institutional cooperation between law enforcement, security and defence, and other actors involved. The rapid evolution of the cyber threats and the complex nature of the institutional landscape has necessitated a number of regulatory policy developments including at EU level.

In the following, we first consider the development of the cybersecurity threats against the EU, and how EU elites have perceived the changing threat landscape, and on this basis articulated the need to expand European cybersecurity policy to tackle the risks. Next, we consider how EU cybersecurity policy has developed in response to these threats and challenges. Finally, we discuss the current challenges for the European Union and discuss the prospects of the currently ongoing regulatory work that will be able to comprehensively and successfully address these challenges.

## The age of hyper-competitiveness and cybersecurity

In her 2021 State of the European Union speech Ursula von der Leyen emphasised that we are facing a new and rapidly developing hyper-competitive security environment, which is characterised by increasing rivalry and competition between powers, where post-Cold War cooperative security options are under attack and the revival of nationalism and protectionism would threaten the stable peace what we have enjoyed in Europe for decades. The words we heard from her were stark and telling: «We are entering a new era of hyper-competitiveness. An era in which some stop at nothing to gain influence: from vaccine promises and high-interest loans, to missiles and misinformation. An era of regional rivalries and major powers refocusing their attention towards each other» (von der Leyen, 2021).

**New emerging security challenges in the much more adversarial present international environment made clear that a rapidly evolving digitalisation does not only offer great boons to our societies but also creates new risks and vulnerabilities.**

The triumph of cooperative and integrationist international political systems that started with the end of Cold War remained short-lived. New emerging security challenges in the much more adversarial present international environment made clear that a rapidly evolving digitalisation does not only offer great boons to our societies but also creates new risks and vulnerabilities. From the attempts to manipulate electoral processes to industrial espionage, hacking classified information from foreign governments, and the potential to cause destruction of enemy infrastructure or military capabilities, cyber threats can no longer be ignored.

Revisionist powers are using cyber-attacks in favour of their strategic ambitions and to challenge the status quo in the international system (Tenembaum, 2012). The world is ushering in a new era of great power rivalry with increasing tensions, in particular trade wars between the United States and a rising power, China. New strategic doctrines have been developed by Russia, China, North Korea, Iran, and other status quo challenging powers, especially about the use of hybrid means to challenging Western dominance. A revisionist power may have an advantage in challenging status quo of the international system because it goes beyond rational expectations (Krastev, 2014). Therefore, the empowerment of some actors and states has caused greater instability and competitiveness in international relations. Moreover, finding durable solutions for global problems like the COVID-19 pandemic or climate change in a strongly polarized international system will likely prove much more difficult than in a system characterised by seeking mutually beneficial outcomes through cooperation.

The rivalry between the United States and China has been intensifying, but with the EU and United States also being potential economic competitors there is also a risk that the unity between Western liberal democracies is undermined by economic tensions.

The recently concluded security and defence pact in September 2021 (AUKUS) between the United States, the United Kingdom and Australia resulted in a diplomatic crisis between Australia and France after Australia dumped the 90 billion AUD contract for French-designed submarines (Sheftalovich, 2021). French Foreign Minister Jean-Yves Le Drian called the announcement of AUKUS "brutal", "unpredictable", and reminiscent of former US president Donald Trump, and Commission President Ursula von der Leyen expressed concern that "one of our member states has been treated in a way that is not acceptable" (Walden, 2021). Those who are challenging the liberal democratic system might capitalise on tensions and disputes between the Western countries.

As new global challenges like the COVID-19 pandemic, the war in Ukraine, or climate change threaten the planet, it would be crucially important that nations work towards joint policies and find appropriate ways to reach comprehensive solutions. In anincreasingly hostile security environment, the European Union remains an area of relative stability characterized by willingness to cooperate and find joint solutions with partners . At the World Health Organization's 73rd assembly in May 2020, Ursula von der Leyen said: «This is the time for cooperation. This is the time for science and solidarity. This is the time for all humanity to rally around a common cause. And you can count on Europe to always play for the team» (von der Leyen, 2020a).

The progress made in moving towards European integration from the Paris Treaty of 1951, which established the European Coal and Steel Community (ECSC), has been impressive and paved the way for closer regional cooperation in a number of fields. It should increase the likelihood that economic-social integration will spill over into political integration, where national governments devolve more authority to the regional organizations (Schmitter, 2004: 47-48). There have been numerous attempts at solving crises in Europe through the EU. For example, following the 2007/2008 financial crisis, the intergovernmental European Stability Mechanism (ESM) was set up to provide lending to Eurozone member states in financial distress (Zeevaert, 2020). In cybersecurity, the allegedly Russian-supported attacks against Estonian governmental institutions and critical infrastructure in 2007 produced a spillover effect that led to further cybersecurity cooperation. Similarly, the COVID-19 pandemic has produced an analogous spillover into health policy.

However, the integrationist approach is looking at rational advantages achieved through enhanced cooperation. The current political climate is

changing and can be disadvantageous for further regional integration. Even as the direct military threat to the European Union coming from other states has been tremendously reduced, we are facing multiple other security challenges like trade wars, uncontrolled migration, refugee crisis, cyberattacks, the deliberate spreading of a "culture of fear", influence operations, status conflicts, social unrests, international terrorism and crime, as well as the risk posed by weapons of mass destruction. These risks could effectively bring an end to what has been achieved since the European integration process started.[1]

Nowadays, cyber is often becoming a marketing term which can be attached practically to everything (Whyte *et al.*, 2021: 4). New technologies have allowed various populist movements from far-right to far-left fringes to use virtual platforms in the dissemination of their ideologies. The rise of social media has allowed these types of movements to acquire an enormous ability to spread their messages. Populist and extremist movements both inside and outside the EU are increasingly propagating an image of a Europe in decline and attempt to discredit liberal democracy by describing it as a "weak" system of government that is in a state of crisis (Krouwel and Önnerfors, 2021). After the election of Donald Trump for the US Presidency in 2016, his more protectionist "America First" programme has encouraged rivalry between great powers and rendered the international system more unstable. The recent populist wave is still strong, and this might confer an advantage to those seeking to undermine and challenge the international system over those that seek to defend it.

An increasing trend is to implement influence operations in the cyber domain, by which certain revisionist governments are targeting the political sentiments or the public discourse in other countries. Computational propaganda has been used for suppressing fundamental human rights, discrediting political opponents, and drowning out dissenting opinions. Liberal democracies may be particularly vulnerable to influence operations, including computational propaganda, because of their free press and freedom of expression tradition gives their opponents an open door to attack their values. A study by Bradshaw and Howard (2019) identified social media manipulations in 70 countries, of which 26 countries were authoritarian-leaning. Seven countries (China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela) used social media platforms (e.g., Facebook, Twitter) for foreign influence operations. According to Bradshaw and Howard, Facebook has been the most popular arena for social media manipulations as 56 countries used this platform for computational

1. And the ongoing Russian-Ukrainian war highlights that military security still needs to be addressed.

propaganda. Studies conducted in Taiwan and Ukraine have demonstrated that long-term media campaigns conducted in newspapers, radio, television, and social media can successfully affect public opinion to increase support candidates endorsed respectively by China or Russia (Baterman *et al.*, 2021).

Cyber operations organised by revisionist actors are intensively targeting knowledge through the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information (Hamulák, 2018). The internet and social media facilitate the spreading of extremist ideologies and conspiracy theories, and highlightsthe dangers posed by digitalisation which could prove damaging to the values of the European Union.

## Cybersecurity challenges

The digital revolution has created a favourable platform for starting and advancing cyberwarfare by the deliberate targeting of computers and networks of sovereign states and international organisations (Troitiño, 2022). In April 2007 the Estonian government moved a World War II memorial commemorating Russian soldiers to a less prominent place in Tallinn, and in response riots among the Russian-speaking minority broke out. Soon after the riots began four waves of cyberattacks, primarily Distributed Denial of Service (DDoS) attacks, were unleashed against Estonian government institutions, media, and banks. While the impact in terms of actual damages on the critical infrastructure was not remarkable, the attack was a "wake-up call" that made Europeans recognise the risks and the need to immediately begin strengthening cybersecurity capabilities.

These developments reached a zenith in the 2021 State of the European Union speech when Commission President von der Leyen emphasised that the nature of contemporary security threats is evolving rapidly by reaching from hybrid or cyber-attacks to the growing arms race in space. «Disruptive technology has been a great equaliser in the way power can be used today by rogue states or non-state groups and there is no need for armies and missiles to cause mass damage. Your laptop or smartphone with internet connection can paralyse industrial plants, city administrations and hospitals and disrupt entire elections with a smartphone and an internet connection» (von der Leyen, 2021).

Cyber-attacks can efficiently target intellectual property, commercial ventures, critical infrastructure as well military systems, but they are also used in information and influence operations to capture the minds of the people and to spread a "culture of fear" and uncertainty. They can affect states, companies, and ordinary citizens with multiple threats to our welfare and safety.

## The terrifying rise of disinformation and fake news in the media landscape

In the contemporary "post-truth"[2] environment, information may easily become a target for manipulations, and exploited by news media looking get more attention and produce profit. There has been rapid advances in terms of artificial production, manipulation, and modification of data and media by automated means, as well as a new wave of deepfakes[3], in which a person in an existing image or video is replaced with someone else's likeness (Kalpokas and Kalpokiene, 2021: 37). The evolution of synthetic media may easily produce misperceptions and promulgate new myths, beliefs, and conspiracies that could for example be exploited help to advance populist parties and ideologies.

## Hacks of government infrastructure

Digitalisation makes attacks against other governments more profitable and concealable as the attacker can easily remain invisible and unidentified. During the COVID-19 pandemic, several EU and national agencies were attacked in the cyber domain. For example, in December 2020 the European Medicines Agency announced that it had been targeted in a cyber-attack. In March 2021 the Dutch newspaper *De Volkskrant* published an article saying "sources close to the investigation" have disclosed that a Russian intelligence agency and Chinese spies were behind the attacks (Reuters, 2021a). Even though this was not confirmed by officials, it does highlight the geopolitical tensions and concerns that rivalling powers can use cyber attacks against Europe.

## Interference to foreign elections

The interference in foreign elections, either through hacks to change the tally, attempts to uncover and then reveal confidential information about a candidate, and various disinformation campaigns, is becoming a constant threat

2. The post-truth world, which describes the situation where "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief," (English Oxford Living Dictionaries, n.d.).
3. Deepfakes are generated by using automated content generation techniques including artificial intelligence to make images of fake events, manipulate or generate text, visual images (e.g. photos-hopping), or audio content (e.g. "cloned voice") (Kalpokas and Kalpokiene, 2021; Sample, 2020).

to democracies. This is also a challenge for Europe. To illustrate, the Russian *Ghostwriter* hacker group was recently found to be targeting members of German elective bodies with fake emails (Cerulus and Klingert, 2021).

## Military application in direct warfare

In 1988, Hashemi Rafsanjani, a speaker of the Iranian Parliament and later President, called chemical and biological weapons a "poor man's atomic bomb" (Headley, 2018). Today his claim can be extended to the potential threat of cyber weaponry. Developing such capabilities is less costly but more efficient. Digital viruses, phishing, computer worms, and malware disseminated by military institutions can take down critical infrastructure and DDoS attacks may harm computer networks and devices (Andress and Winterfeld, 2014).

## Cyber-espionage

In the public perception, cyber-attacks are often associated with attacks against countries with the purpose of harming their critical infrastructures, but digitalisation has also opened new ways to get access to new technologies and business secrets. Anonymous cyber espionage campaigns targeted several government officials including the Belgian interior minister, Polish politicians, and hospitals in Ireland and France (Cerulus, 2021a). Concerns over Chinese involvement in 5G wireless networks stem from allegations that cellular network equipment sourced from Chinese vendors may contain backdoors that would enable the Chinese government to establish surveillance of the users.

## Economic warfare, industrial espionage, and the decoupling dilemma

This may include industrial espionage (e.g., theft of intellectual property, confidential information, various commercial plans), pressure and threats on clients and simply trying to stir up trouble to damage competitors. The US Trump administration issued an executive order about restricting transactions of information communication technology (ICT) products or services linked to a "foreign adversary", which is related to accusation that Chinese companies (e.g., Huawei) use their products for industrial espionage (Lim and Ferguson, 2019). The issue is also related to criminal actions, which under certain circumstances may involve the state itself. For example, North Korea is getting an estimated

share of their revenue from cyber theft (Reuters, 2019), which is becoming a sort of business model for rogue states, but also for unrecognised international actors (e.g., the Islamic State).

### Crime in cyberspace

Cyber criminals do not have to steal secret papers and blueprints from locked safes but can simply hack into the computer systems of their rivals. Recent reports indicate that cybercrime is getting better organised and becoming more widespread. This damages European companies, large and small, and threatens to undermine trust in the digital economy. It is worth mentioning that 43% of cyber-attacks target small businesses, which obviously have less the resources and financial capabilities to invest in cybersecurity (Cyber Competence Network, 2021).

By all accounts we have only seen the top of the iceberg of what cybersecurity actors need to be ready to deal with in the near future as they have to address situations of heightened geopolitical tensions which could lead to massive spikes in the number of incidents and full-fledged cyber-attacks.

## The development of EU policy in response to growing cybersecurity challenges

The EU's work in cybersecurity can be traced back to 2004 when the European Network and Information Security Agency (ENISA) was set up in Heraklíon, Greece. Its responsibilities included conducting analysis and research on cybersecurity, fostering cooperation and trust among EU member states in the field, and providing training and contributing to awareness-raising[4]. It took almost a decade for the next major cybersecurity development in the European Union to occur. EU-LISA (European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice) was established in 2011 to manage the large-scale IT systems needed for, in particular, Schengen, and the European Border and Coast Guard Agency

4. Regulation (EC) No 460/2004 .

(Frontex). In 2013 the European Union unveiled its first cybersecurity strategy, which in its threat assessment described a diversity of risks arising from state-sponsored cyber activities[5] to political or criminal groups.

The cybersecurity strategy strongly emphasised the importance of the work on the so-called Network and Information Security (NIS) directive (Directive (EU) 2016/1148). NIS would establish common minimum requirements around cybersecurity across the EU Member States and ensure coordination by setting up contact bodies to engage in relevant networks and liaise with ENISA and the European Commission. Political agreement on the NIS directive[6] was reached in December 2015, and the final directive was adopted and entered into force in July 2016. It gave the EU Member States 21 months to fully transpose its requirements into national legislation, although in fact full implementation was not deemed complete until 2020.

**In 2013 the European Union unveiled its first cybersecurity strategy, which emphasised the importance of the work on the so-called Network and Information Security (NIS) directive, which would establish common minimum requirements around cybersecurity across the EU Member States and ensure coordination by setting up contact bodies to engage in relevant networks and liaise with ENISA and the European Commission.**

NIS also developed an institutional structure for the EU's work within cybersecurity. Member States have been required to designate points of contact for information-sharing with the other member states and the EU institutions to monitor and ensure the implementation of the legal requirements of the NIS Directive. They were also to set up Computer Security Incident Response Teams (CSIRT) to monitor incidents at national level and work together through a CSIRT network to facilitate cooperation and information-sharing. Finally, Member States were to appoint a national representative to a Cooperation Group which would be set up to deal with the broad range of issues around cybersecurity in the EU.

Meanwhile Europol, the EU's agency for legal enforcement and police cooperation, opened a new European Cybercrime Centre (EC3) in 2013. Combining research into cybercrime threats with operational cooperation, EC3 provides a locus for cooperation between member state services whilst offering

5. But note, "state-sponsored" presupposes the understanding that foreign states would not be directly involved.
6. formally, directive Concerning measures for a high common level of security of network and information systems across the Union (European Union, 2016).

analytical including technical and digital forensic support to investigations. Eurojust (the European Union Agency for Criminal Justice Cooperation) has also gradually assumed a coordinating role in legal cases and judicial matters involving cybersecurity, and the European Defence Agency (EDA) has developed training programmes, carried out exercises[7] and conducted research within the cyber domain (European Defence Agency, 2021b).

In 2015 the EU unveiled a new strategic document, "The European Agenda on Security", which took a broad look at security challenges faced by Europe and listed cybersecurity as one of three key priorities which required coordination at EU level. In 2017, the European Commission released an updated version of its cybersecurity strategy (RTE, 2017). The strategy encapsulated a changing view of the landscape with then-Commission President Jean-Claude Juncker noting in his 2017 State of the Union speech that «Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. (…) This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks» (Juncker, 2017). Equivalating cybersecurity with "real world" kinetic security was an important step in the development of EU cybersecurity policy from a niche to a mainstream topic as it suggested a heightened threat perception.

**In 2017, the European Commission released an updated version of its cybersecurity strategy which encapsulated a changing view of the landscape with then-Commission President Jean-Claude Juncker noting in his 2017 State of the Union speech that «Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. (…)».**

In order to implement the strategic designs in the updated Cybersecurity strategy the Commission also put forward the so-called Cybersecurity Act in 2017 and a so-called "cyber diplomacy toolbox", or more formally a "Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities" (Bendiek *et al.*, 2017). ENISA had hitherto only a temporary mandate which was dependent on political and fiscal support to renew it, that was frustrating attempts at longer-term planning. The Cybersecurity Act finally gave ENISA a

7. For example, EU CYBRID in September 2017, organised by the Estonian Presidency of the Council of the European Union, was first cyber exercise at EU ministerial level that aimed in particular at raising awareness of cybersecurity incident coordination and strategic decision-making, (Kerikmäe *et al.*, 2019)

permanent mandate and expanded the scope of its operational responsibilities. Importantly ENISA was also assigned the responsibility for the roll-out of EU cybersecurity certification schemes (which includes a number of initiatives, for example common standards for industry cloud computing).

The EU has been called a "regulatory superpower" (Bradford, 2020) and a "economic giant, but political dwarf" (see e.g. Leonard, 2018). As such the European Union may find it difficult to develop a decisive role in the highly politicized field of security policy, but should be well posited to employ its regulatory and economic power to establish cybersecurity related certification and standardisation schemes with widespread uptake. Important work is ongoing in the field, for example with agreement reached in January 2020 on establishing a new "5G Toolbox" for 5G cybersecurity classifications (ENISA, 2020). This work is crucial to ensuring sufficient cybersecurity standards in Europe especially in light of the growth of e.g., Internet of Things technology becoming more widespread, and may also help stimulate the growth of a European cybersecurity industry.

Accompanying the updated strategy and Cybersecurity Act the Commission also issued a "Blueprint for coordinated response to large-scale cybersecurity incidents and crises at the Union level" (European Commission, 2017) and put forward a Cybersecurity Toolbox which essentially had foreign ministers consenting that "restrictive measures" (i.e. EU sanctions) could be deployed in response to "malicious cyber activities". This option would later be put to use in July 2020 when the EU imposed its first-ever sanctions, travel ban and asset freeze targeting six individuals from China and Russia, and three entities from China, Russia and North Korea, in response to a number of incidents including the much-publicised "WannaCry" attack (Official Journal of the European Union, 2020b), and later complemented by asset and travel ban sanctions targeting the Russian military unit, colloquially known as "Fancy Bear", and two individuals from that unit, for the 2015 hack of the German parliament (Official Journal of the European Union, 2020a).

In late 2019, upon assuming the mantle of President of the European Commission, Ursula von der Leyen declared the digital transition (together with the green transition) to be the main focus for her mandate, setting the scene for a spate of legislatives initiatives around digital policy including in the cyber domain (von der Leyen, 2020b). In mid-2019 she put forward the Political Guidelines, which describes the aims and visions of each new Commission, outlining the intention to set up a Joint Cyber Unit. In December 2020 the European Commission published a new cybersecurity strategy. The threat landscape it described was darker, and the number of initiatives foreseen in the new strategy much more comprehensive, than its 2013 predecessor.

The 2020 cybersecurity strategy called for a revision of the NIS directive, which an impact assessment had found to have been implemented very differently across the EU member states leading to a fragmentation of security standards and practices. The revised so-called "NIS2" directive would broaden the scope by covering all medium-sized and large companies within a larger range of sectors (with additional sectors such as telecom now included), and also cover small enterprises insofar as they are deemed to have a high security risk profile. The directive would streamline the requirements imposed on the covered companies, including with legal obligations to notify cybersecurity incidents to relevant authorities within fixed timeframes (European Commission, 2020b). NIS2 will move further towards harmonising sanctions across member states and will also set up an EU registry of vulnerabilities at ENISA (European Commission, 2020b). The European Cyber Crisis Liaison Organization Network, EU-CyCLONe,[8] will be established to provide cooperation between member states around crisis incidents (ENISA, 2021).

**In December 2020 the European Commission published a new cybersecurity strategy which described a darker threat landscape, foresaw a much more comprehensive number of initiatives, and called for a revision of the NIS directive.**

As part of the cybersecurity package, the Commission also put forward a proposal for a Directive on the resilience of critical entities, the so-called CER directive (European Commission, 2020d). The CER directive seeks to strengthen resilience of actors deemed critical to the workings of an organised society by expanding scope and obligations and strengthening cross-border cooperation. As proposed by the Commission it will also go beyond the scope in the existing Directive on Critical Infrastructure by not only covering energy, and transport, but also banking, financial markets, public administration and space. The directive requires Member States to identify critical entities, to lay down a strategy for reinforcing their resilience, to regularly assess the risks that may affect them, and set up obligations for critical entities to ensure their resilience, with the directive listing a number of measures that such entities should undertake to increase resilience.

Complementing these legislative actions, the cybersecurity strategy also calls for a number of institutional developments: the development of an EU DNS[9]

8. The network was established in 2021 building on French-Italian cooperation to provide liaison between the technical level i.e., CSIRTs and the political level during large-scale cyber-related crises (ENISA, 2020).
9. Domain Name Systems (DNS) are key to the functioning of the modern internet and the EU is concerned about disruptions or attacks against one or more of the key corporate providers.

resolver service, new secure quantum communications infrastructure (QCI) for public authorities to transmit confidential information, and stronger cybersecurity for the European Institutions themselves (with a regulation underway to update the current rules). Perhaps most importantly the Commission intends to set up a "Cyber Shield", a network of Security Operations Centres across the EU to detect threats very fast and allow for proactive actions before damages including by making use of artificial intelligence (European Commission, 2020c).

The EU is simultaneously moving ahead with a number of non-horizontal legislative initiatives that will have important bearings on cybersecurity. This will include new rules for energy operators, new rules concerning cross-border electricity flow and energy infrastructure, and a directive "The EU's Digital Operational Resilience Act for financial services (DORA) (Krüger and Brauchle, 2021).

The EU is therefore preparing new institutional developments in an already complex cybersecurity landscape, with a Joint Cyber Unit to be set up in Brussels, and a new European Cybersecurity Competence Centre being established in Bucharest. Complementing these EU institutional developments, a private-sector European Cyber Security Organisation (ECSO) has been established to work with the EU on public-private partnerships around cybersecurity. Since every agency, business, and citizen uses digital tools in some form or another, cybersecurity is also to some extent integral to every sector and policy area. The result is that the number of actors working within EU cybersecurity is large and still growing and involves a large number of Directorate-Generals (DG's) and specialized EU agencies. Similarly legislative initiatives in other areas increasingly overlap with cybersecurity, such as the work to address the legal responsibilities of online intermediaries e.g., social media through the new Digital Services Act (DSA), which will also have important ramifications for the spread of disinformation within Europe (Krüger and Brauchle 2021). In the same vein the EU is preparing to deploy budgetary resources from a variety of EU programmes and sources with different scopes and objectives to bolster its work on cybersecurity. Along with investments from Member States, the European Commission expects a total of up to €4.5 bn to be mobilized for investments in cybersecurity over the period 2021-27.[10]

10. Overview of cybersecurity policies in the EU Domenico Ferrara, Policy Officer European Commission, DG CNECT.H.1 Cybersecurity Technology and Capacity Building (in Gonzalez-Sancho, 2021)

The implication is that in order to successfully tackle cybersecurity threats, effective coordination and liaison between a large number of actors and institutions at varying levels will be necessary (Singh, 2018; Ilves et. al., 2016).

## Challenges and issues in the evolving EU cybersecurity framework

One notable conclusion that arises out of the 2020 cybersecurity strategy is that the EU is striving to be able to "prevent, discourage, deter and respond effectively" to cyber-attacks (European Commission, 2020c), but in order for cybersecurity capabilities to act as effective deterrence they must by implication be potentially employed for offensive use as well. This marks a significant deviation from the EU's traditional posture in security policy and inevitably raises a number of questions about the roles between the EU, NATO and the EU Member States themselves in a complex, multi-layered landscape with many actors (European Court of Auditors, 2019).

**One notable conclusion that arises out of the 2020 cybersecurity strategy is that the EU is striving to be able to "prevent, discourage, deter and respond effectively" to cyber-attacks, but in order for cybersecurity capabilities to act as effective deterrence they must by implication be potentially employed for offensive use as well. This marks a significant deviation from the EU's traditional posture in security policy.**

Cybersecurity encompasses a number of spheres and ranges from regular crime and criminal investigations to the actions of foreign states, and from phishing and CEO fraud to hacking, securing information, disabling systems and spreading disinformation. The EU therefore needs to routinely secure coordination and liaison between not only the Commission and its agencies, but also the 27 Member States, as well as external partners (e.g. NATO in matters pertaining to defence and military security) (Carrapico and Barrinha, 2017). But whilst the EU has been able to set up a large array of cybersecurity contact points, networks, and agencies, it does not necessarily ensure that they reach an effective operational capacity (European Court of Auditors, 2019). Moreover, achieving seamless information exchange and effective cooperation is challenging across this complex landscape. Further confounding matters is the fact that relations with NATO are not necessarily characterised by a high degree

of trust, especially following instances of US spying against European allies, or by a clear and mutually reinforcing division of tasks and responsibilities in the emerging cybersecurity field (Reuters, 2021b). Also complicating the situation is that EU member states have so far proven recalcitrant towards any aspirations for stronger EU cooperation and integration within security and defence matters, as many prefer to keep full national sovereignty over such matters or keep cooperation within NATO rather than the EU.

In contrast, revisionist powers that can potentially target EU countries tend to have a much greater unity of organisation and direction than the multi-institutional setup characterising Europe, which potentially puts the Europeans at a disadvantage. A controversial topic in recent years has been that the Chinese tech and 5G giant, Huawei, may be constructing "backdoors" into its systems and hardware which could be used for infiltrating (Pancevski, 2020). This has led to the United States to ban Huawei and attempt to convince the Europeans to do likewise .

European policymakers can no longer ignore risks posed by foreign ownership of digital infrastructure and must decide which regulatory steps might be appropriate to take to curb such dependencies and risks. EU member states have taken various positions in response to in particular the allegations made against Huawei, but with the direction of travel being towards more restrictive measures (Cerulus, 2021b), combined with initiatives to lessen external dependencies such as the recent launch of a European Alliance for Industrial Data, Edge and Cloud. Reflecting these policy discussions and developments the EU has put in place a Foreign Direct Investment Screening Regulation[11] to provide a framework for coordination around national investment screening, i.e. that foreign investments can be blocked out of national security concerns (European Commission, 2020a). Regardless, the issue of foreign investments and the access of foreign companies to key technologies will continue to be a thorny issue at the forefront of EU cybersecurity debate in the coming years.

The EU must manage a context with a large number of actors and institutions that will have to work together to ensure effective cybersecurity efforts throughout Europe. It must also navigate in a context where cybersecurity is moving fast from niche to mainstream, from a policy area for specialists to one of acute political importance at the top of the political agenda. It must also handle growing unease about being dependent on foreign vendors of technological solutions, as well as the increasingly difficult issue of the free flow

11. Regulation (Eu) 2019/452 of The European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union

of data, including a trend towards the regionalisation of internets (Chernaskey 2021; Sherman, 2019).

## Conclusions

The EU has responded to the rapid proliferation of cybersecurity threats by adapting and widening its strategic perception. This began in 2013 when the EU unveiled its first cybersecurity strategy and has continued over the past decade, culminated with a new ambitious strategy launched in December 2020 and reiterated in von der Leyen's 2021 State of the Union speech. In response to the changing threat perception, the EU has developed an institutional setup with a full-fledged cybersecurity agency, various networks, contact points, and coordinating bodies, and is now going further with new initiatives such as plans to set up a "Cyber Shield" to provide a high level of security for the EU and its member states. At the same time, the EU has worked to set up a regulatory regime with a number of directives establishing common standards and rules, and is also working on certification and standardisation schemes

**For the EU, finding a suitable division of responsibilities and a modus vivendi that ensures effective cooperation between this large number of actors at different levels will be difficult, but vital to ensuring an appropriate response in Europe to the growing cyber threat.**

Cybersecurity nevertheless will remain a difficult subject for the EU in the coming years. Even though it is a large "regulatory power", it has remained a relatively insignificant player in security policy issues which many member states prefer to handle themselves or within NATO. Cybersecurity ranges from judicial and operational law enforcement cooperation to actual military defence against other states or state-sponsored groups. Finding a suitable division of responsibilities and a modus vivendi that ensures effective cooperation between this large number of actors at different levels will be difficult, but vital to ensuring an appropriate response in Europe to the growing cyber threat.

### Bibliographical references

Andress, Jason;Winterfeld, Steve. *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners*. Elsevier Inc., 2014 DOI: https://doi.org/10.1016/C2013-0-00059-X

Bateman, Jon; Hickok, Elonnai;Shapiro, Jacob N. «Measuring the Effects of Influence Operations: Key Findings and Gaps from Empirical Research». *Carnegie Endowment for International Peace*. (28 June 2021). (online) [Date retrieved: 30.09.2021] https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824

Bendiek, Annegret; Bossong, Raphael;Schulze, Matthias. «The EU's Revised Cybersecurity Strategy». *Stiftung Wissenschaft und Politik*. SWP Comments no. 47, 2017 (online) [Date retrieved: 01.10.2016] https://www.swpberlin.org/publications/products/comments/2017C47_bdk_etal.pdf

Bradford, Anu. «When It Comes to Markets, Europe Is No Fading Power. The EU Sets the Standards for the Rest of the World». *Foreign Affairs*, (3 February 2020) (online) [Date retrieved: 11.09.2021] https://www.foreignaffairs.com/articles/europe/2020-02-03/when-it-comes-markets-europe-no-fading-power

Bradshaw, Samantha;Howard, Philip N. «The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation». *Working Paper*. Oxford, UK: Project on Computational Propaganda, 2019. (online) [Date retrieved 12.09.2021] https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Carrapico, Helena;Barrinha, André. «The EU as a Coherent (Cyber)Security Actor?». *Journal of Common Market Studies*, vol. 55, no. 6, pp. 1254-1272, 2017. DOI: https://doi.org/10.1111/jcms.12575

Cerulus, Laurens (a). «EU to launch rapid response cybersecurity team». *Politico* (21 June 2021). (online) [Date retrieved 02.10.2021] https://www.politico.eu/article/eu-joint-cyber-unit-rapid-response-cyberattacks/

Cerulus, Laurens (b). «Germany falls in line with EU on Huawei». *Politico.* (23 April 2021) (online) [Date retrieved 02.10.2021] https://www.politico.eu/article/germany-europe-huawei-5g-data-privacy-cybersecurity/

Cerulus, Laurens;Klingert, Liv. «Russia's 'Ghostwriter' hacker group takes aim at German election». *Politico*. (21 September 2021) (online) [Date retrieved 02.10.2021] https://www.politico.eu/article/russia-brash-hackers-turn-to-german-election/

Chernaskey, Rachel. «The World Wide Web's Break Up: State-Backed Media's Role in Supporting Internet Fragmentation». *Foreign Policy Research Institute (fpri.org)* (28 February 2021) (online) [Date retrieved 30.09.2021] https://www.fpri.org/fie/internet-break-up-russia-china/

Cyber Competence Network. «Four EU pilot projects to prepare the European Cybersecurity Competence Network». (2021) (online) [Date retrieved 30.09.2021] https://cybercompetencenetwork.eu/about/

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. [Date retrieved 12.09.2021] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

*English Oxford Living Dictionaries*. (online) [Date retrieved 04.08.2021] https://en.oxforddictionaries.com/definition/post-truth

Eurojust. «Overview Report Challenges and best practices from Eurojust's casework in the area of cybercrime». (2020). (online) [Date retrieved 04.10.2021] https://www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_Cybercrime-Report.pdf

European Commission (a). «Decision on establishing the office of the European Network and Information Security Agency (ENISA) in Brussels». (22 June 2021) (online) [Date retrieved 04.10.2021] https://digital-strategy.ec.europa.eu/en/news/decision-establishing-office-european-union-agency-cybersecurity-enisa-brussels

European Commission (b). «Joint Cyber Unit». (23 June 2021) (online) [Date retrieved 04.10.2021] https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

European Commission (b). «Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union». (16 December 2020) (online) [Date retrieved 04.10.2021] https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union

European Commission (c). «New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient». (16 December 2020) (online) [Date retrieved 04.10.2021] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

European Commission (d). «The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU». (16 December 2020) (online) [Date retrieved 04.10.2021] https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential_en

European Commission (e). «EU foreign investment screening mechanism becomes fully operational». *Press Release* (9 October 2020) (online) [Date retrieved 04.10.2021] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867

European Commission. «COMMISSION RECOMMENDATION (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises». (13 September 2017) (online) [Date retrieved 04.10.2021] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN

European Council. «EU imposes the first ever sanctions against cyber-attacks». *Press Release* (30 July 2020) (online) [Date retrieved 30.09.2021] https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

European Court of Auditors. «Challenges to effective EU cybersecurity policy». *Briefing Paper* (March 2019), (online) [Date retrieved 04.10.2021] https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

European Defence Agency (2021). «EDA's Growing Role in Cybersecurity». *European Defence Matters*, issue 18, 2021 (online) [Date retrieved 04.10.2021] https://eda.europa.eu/webzine/issue18/focus/eda-s-growing-role-in-cybersecurity

European Medicines Agency. Cyberattack on EMA – update 5». (15 January 2021) (online) [Date retrieved 04.10.2021] https://www.ema.europa.eu/en/news/cyberattack-ema-update-5

European Network and Information Security Agency. «EU Member States test rapid Cyber Crisis Management». *Press Release* (19 May 2021) (online) [Date retrieved 04.10.2021] https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-rapid-cyber-crisis-management

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union». *Official Journal of the European Union*, (19 July 2016) (online) [Date retrieved 12.09.2021] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

European Union Agency for Cybersecurity. «EUCS – Cloud Services Scheme» (22 December 2020) (online) [Date retrieved 04.10.2021] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/

European Union Agency for the Cooperation of Energy Regulators. «Framework Guidelineonsector-specificrulesforcybersecurityaspectsofcrossborderelectricity flows». (22 July 2021) (online) [Date retrieved 04.10.2021] https://documents.acer.europa.eu/Official_documents/Acts_of_the_Agency/Framework_Guidelines/Framework%20Guidelines/Framework%20Guideline%20on%20Sector-Specific%20Rules%20for%20Cybersecurity%20Aspects%20of%20Cross-Border%20Electricity%20Flows_210722.pdf

Gonzalez-Sancho, Miguel. «Standardisation supporting the Cybersecurity Act». *ENISA Cybersecurity standardization conference 2021* (3 February 2021) (online) [Date retrieved 30.09.2021] https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/presentations/03-04-gonzalez-sanchoHamulák, O. (2018). La carta de los derechos fundamentales de la union europea y los derechos sociales. *Estudios constitucionales*, *16*(1), 167-186.

Headley, Tyler. «Introducing 'the Poor Man's Atomic Bomb': Biological Weapons». *National Interest*, (2 December 2018) (online) [Date retrieved 04.10.2021] https://nationalinterest.org/blog/buzz/introducing-poor-mans-atomic-bomb-biological-weapons-37437

Ilves, Luukas K.; Evans, Timothy J.; Cilluffo, Frank J.;Nadeau, Alec A. «European Union and NATO Global Cybersecurity Challenges: A Way Forward». *PRISM*, Vol. 6, No. 2, pp. 126-141, 2016.

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions. «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace». (2013) (online) [Date retrieved 04.10.2021] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

Juncker, Jean-Claude. «State of the Union Address». (13 September 2017) (online) [Date retrieved 04.08.2021] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165

Kalpokas, I.;Kalpokiene, J. (2021). Synthetic media and information warfare: Assessing potential threats. In *The Russian Federation in Global Knowledge Warfare* (pp. 33-50). Springer, Cham.

Kerikmäe, T.,;Troitiño, D. R.; Shumilo, O. (2019). An idol or an ideal? A case study of Estonian e-Governance: Public perceptions, myths and misbeliefs. *Acta Baltica Historiae et Philosophiae scientiarum*, *7*(1), 71-80.

Krastev, Ivan. «Putin's world». *Project Syndicate* (1 April 2014) (online) [Date retrieved 30.04.2019] www.project-syndicate.org/commentary/ivan-krastev-blamesthe-west-s-weak-response-in-crimea-for-empowering-russia#AK0vzVbmtIUQCseG.99

Krouwel, Andre; Önnerfors, Andreas (Eds). *A Continent of Conspiracies: Conspiracy Theories in and about Europe*. Abingdon-on-Thames, England, UK: Routledge, 2021. DOI: 10.4324/9781003048640

Krüger, Philipp S.;Brauchle, Jan-Philipp. «The European Union, Cybersecurity, and the Financial Sector: A Primer». *Carnegie Endowment for International Peace* (16 March 2021) (online) [Date retrieved 12.09.2021] https://carnegieendowment.org/2021/03/16/european-union-cybersecurity-and-financial-sector-primer-pub-84055

Leonard, Mark. «Europe for itself». *European Council of Foreign Relations* (24 July 2018) (online) [Date retrieved 12.09.2021] https://ecfr.eu/article/commentary_europe_for_itself/

Lim, Darren; Ferguson, Victor. «Huawei and the decoupling dilemma». *The Interest*. (2019) [Date retrieved 30.09.2021] https://www.lowyinstitute.org/the-interpreter/huawei-and-decoupling-dilemma

Maurer, Lucas. «Europe in the post-COVID-19 world». *Atlantic files* (19 May 2021) (online) [Date retrieved 22.07.2021] https://www.orfonline.org/expertspeak/europe-post-covid19-world/

NATO (a). «Brussels Summit Communiqué». (14 June 2021) (online) [Date retrieved 30.09.2021] https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en

NATO (b). «Cyber defence». (2 July 2021) (online) [Date retrieved 30.09.2021] https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en

Official Journal of the European Union (a). «Of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States». L 351 I (22 October 2020), (online) [Date retrieved 30.03.2022] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2020:351I:FULL&from=FR)

Official Journal of the European Union (b). «Amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States». L 246 12 (30 July 2020), (online) [Date retrieved 30.03.2022] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN

Pancevski, Bojan. «U.S. Officials Say Huawei Can Covertly Access Telecom Networks». *The Wall Street Journal* (12 February 2020) [Date retrieved 04.10.2021] https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256

PESCO. «Cyber exercise provides readiness to respond to cyber threats». *Press Statement* (28 May 2021) (online) [Date retrieved 30.09.2021] https://pesco.europa.eu/wp-content/uploads/2021/05/PRESSSTATEMENT-CRRT.pdf

Regulation (EC). «No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency». (10 March 2004) [Date retrieved 30.09.2021] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union

Reuters (a). «Russian, Chinese hackers targeted Europe drug regulator: newspaper». (6 March 2021) (online) [Date retrieved 03.10.2021] https://www.reuters.com/article/us-eu-cyber-idUSKBN2AY0F1

Reuters (b). «U.S. spied on Merkel and other Europeans through Danish cables - broadcaster DR». (30 May 2021) (online) [Date retrieved 30.09.2021] https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/

Reuters (c). «North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report». (5 August 2019) (online) [Date retrieved 03.10.2021] https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX

RTE. «Plans unveiled for EU to step up cyber security efforts». (19 September 2017) (online) [Date retrieved 12.09.2021] https://www.rte.ie/news/2017/0919/905989-eu-cybersecurity

Sample, Ian. «What are deepfakes – and how can you spot them?». *The Guardian* (13 January 2020) (online) [Date retrieved 03.10.2021] https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

Schmitter, Philippe C. «Neo-Neofunctionalism». In: Diez, T.; Wiener, A. (eds) *European Integration Theory*. Oxford: Oxford University Press, pp. 45-75, 2004.

Sheftalovich, Zoya. «Why Australia wanted out of its French submarine deal». *Politico* (16 September 2021) (online) [Date retrieved 12.03.2022] https://www.politico.eu/article/why-australia-wanted-out-of-its-french-sub-deal/

Sherman, Justin. «Russia and Iran Plan to Fundamentally Isolate the Internet». *Wired* (6 June 2019) (online) [Date retrieved 09.10.2021] https://www.wired.com/story/russia-and-iran-plan-to-fundamentally-isolate-the-internet

Singh, Rajnish. «Cybersecurity: Defending the digital wall». *The Parliament Magazine* (4 June 2018) (online) [Date retrieved 30.09.2021] https://www.theparliamentmagazine.eu/news/article/cybersecurity-defending-the-digital-wall

Tenembaum, Yoav D. «International Relations: It's Time to Revise How We Talk About Revisionist Powers». *OXPOL. The Oxford University Politics Blog* (6 November 2012) (online) [Date retrieved 22.07.2021] https://blog.politics.ox.ac.uk/internationalrelations-its-time-to-revise-how-we-talk-about- revisionist-powers/

Troitiño, D. R. (2022). The European Union Facing the 21st Century: The Digital Revolution. *TalTech Journal of European Studies*, *12*(1), 60-78.

von der Leyen, Ursula. «Speech at World Health Organization's 73rd Assembly». (19 May 2020) (online) [Date retrieved 30.09.2021] https://ec.europa.eu/commission/presscorner/detail/en/speech_20_916

von der Leyen, Ursula. «State of the Union Address». (16 September 2020) (online) [Date retrieved 30.09.2021] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

von der Leyen, Ursula. «State of the Union 2021». (15 September 2021) (online) [Date retrieved 30.09.2021] https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2021_en

Walden, Max. «How can Australia repair its relationship with France after the AUKUS submarine row?». *ABC News* (23 September 2021) (online) [Date retrieved 04.10.2021] https://www.abc.net.au/news/2021-09-23/how-can-australia-repair-its-relationship-with-france-aukus/100480270

Whyte, Christopher; Thrall, A. Trevor;Mazanec, Brian M. (eds). *Information Warfare in the Age of Cyber Conflict*. Abingdon-on-Thames, England, UK: Routledge, 2021. DOI: https://doi.org/10.4324/9780429470509

Zeevaert, Marius. «Spillovers versus Bargaining – Which Integration Theory Explains the EU's Coronavirus Recession Response?». *The Yale Review of International Studies* (October 2020) (online) [Date retrieved 30.09.2021] http://yris.yira.org/global-issue/4325#_ftn8