BRIEFING

EU policies – Insights

# Understanding the EU's approach to cyber diplomacy and cyber defence

## SUMMARY

Despite its expertise in cyber public awareness campaigns, research and development, and educational programmes, the EU is still subject to constant cyber attacks. The EU's response to a sophisticated cyber threat spectrum is comprehensive, but perhaps the most *European* aspect of its toolbox is cyber diplomacy. Cyber diplomacy aims to secure multilateral agreements on cyber norms, responsible state and non-state behaviour in cyberspace, and effective global digital governance. The goal is to create an open, free, stable and secure cyberspace anchored in international law through alliances between like-minded countries, organisations, the private sector, civil society and experts. Cyber diplomacy coexists with its sister strands of cyber defence, cyber deterrence and cybersecurity.

Offensive cyber actors are growing in diversity, sophistication and number. Disruptive technologies powered by machine-learning and artificial intelligence pose both risks and opportunities for cyber defences: while attacks are likely to increase in complexity and make attribution ever more problematic, responses and defences will equally become more robust. Burning issues demanding the international community's attention include an emerging digital arms race and the need to regulate dual-use export control regimes and clarify the rules of engagement in cyber warfare.

Multilateral cyber initiatives are abundant, but they are developing simultaneously with a growing push for sovereignty in the digital realm. The race for cyber superiority, if left unchecked, could develop into a greater security paradox. The EU's cyber diplomacy toolbox and its bi- and multilateral engagements are already contributing to a safer and more principled cyberspace. Its effectiveness however hinges on genuine European and global cooperation for the common cyber good. Ultimately, the EU's ambition to become more capable, by becoming 'strategically autonomous' or 'technologically sovereign', also rests on credible cyber defence and diplomacy.

In this Briefing



EPRS | European Parliamentary Research Service

Author: Tania Lațici. Graphics: Samy Chahri.
Members' Research Service

PE 651.937 – May 2020

EN

# The art of cyber diplomacy

'The supreme art of war is to subdue the enemy without fighting', wrote ancient Chinese military strategist Sun Tzu in *The Art of War*. In the cyber realm, the preferred EU alternative to cyber warfare is diplomacy and cooperation. This is best shown in the 2016 EU Global Strategy (EUGS), which describes the aims and conditions of cyber diplomacy. The Strategy explicitly seeks 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 alliances between like-minded countries, organisations, the private sector, civil society and experts.

Cyber capacity and confidence-building with partners – pillars of cyber diplomacy – are duly emphasised. The central elements of capacity and confidence-building measures in cyberspace, according to European Commission guidance, can be summarised as follows:

- developing and building the resilience of institutions able to respond to and recover from cyber threats;
- securing diplomatic commitments to uphold an open, free and safe cyberspace;
- promoting inclusive growth and the sustainable development of digital infrastructure;
- improving digital markets and securing a safe online economy;
- developing cyber defence strategies to protect military networks, assets and defence institutions.

The Organization for Security and Co-operation in Europe (OSCE) has spearheaded progress on cyber confidence-building measures by adopting a framework of 16 guiding measures. The EU has expressed support for these voluntary measures. Yet as one study argues, some countries are still hostile to the idea of a 'central global regulatory body for security in cyberspace' with concerns about loss of national sovereignty. Centralised or not, cyber diplomacy among like-minded countries and organisations is key to the process of attributing who the perpetrator of an attack is. The creation of a complete picture depends on the respective national and international bodies sharing information and analyses to put the pieces together. The accuracy of the picture also depends on the extent to which the private sector is involved, as it could hold a lot of elucidatory data and expertise. The study concludes by assessing how cyber diplomacy tools could become a force for peace by upholding 'international norm building, data protection and freedom of expression, internet governance, and prosecution under international agreements'.

Cyber diplomacy can also be understood as a means of de-escalation. For example, in spring 2019 in response to Iranian provocation in the Persian Gulf, the United States (US) ordered an offensive cyber operation. In this case, the cyber counter-reaction was preferable to deploying troops and risking a major escalation. Correspondingly, an Atlantic Council study explains how 'cyber operations have tended to offer great powers escalatory offramps' without engaging military forces.

Reference is often made to the Tallinn Manual in the context of cyber diplomacy efforts. Coordinated by the Cooperative Cyber Defence Centre of Excellence (CCDCoE) of the North Atlantic Treaty Organization (NATO), there have so far been two editions of the Tallinn Manual, the latest in 2017. It is an expert-driven product, based on consultations between international law scholars and practitioners. The most comprehensive analysis of its kind, the manual addresses the applicability of existing international law to cyber warfare, with a particular focus on attacks falling below the armed conflict threshold.

Some nevertheless argue that despite entrusting almost everything to cyberspace, from personal data to critical infrastructure, governments have fallen short in defending it, or that 'no country or organisation is 'cyber ready'', reaffirming the need for joint, global cyber cooperation. Others point out that multilateral stakeholders' general preference for a minimally regulated cyberspace might lead to a 'fragmentation of cyberspace and future technologies'. If a push for 'cyber sovereignty' continues, global interconnectivity, cooperation and interoperability could be disrupted. While it has been determined that international law does apply to cyberspace, states still disagree about how it applies in instances such as self-defence, adopting counter-measures and situations falling under international humanitarian law. The EU approach rests as much on cyber diplomacy measures

as it does on cyber defence and deterrence. The EU and its Member States recognise the importance of investing in robust defences nationally and across Europe to protect assets and to dissuade potential perpetrators. At the same time, they are also prioritising international cooperation on cyber norms, resilience and responsible behaviour. This approach adheres to the principle: a chain is only as strong as its weakest link.

## Cyber defence: The silent hero

Cyberspace is now considered the fifth domain of warfare alongside the traditional, sea, land, air and space. It is a domain encompassing everything from information and telecommunication networks, infrastructure, and the data they support, to computer systems, processors and controllers. The increasingly hostile use of information and communication technology (ICT) tools via cyber attacks has resulted in the politicisation of this domain since the 1990s and prompted the emergence of the sub-fields of cyber defence and cyber diplomacy. The diversity of cyber threats has increased over time to include anything from outright cyber conflict or warfare, to cyber sabotage and espionage. The umbrella term cyber attack generally covers all types of cyber crime, from defacing a website to targeting electoral campaigns.

It is estimated that roughly one million additional people join the internet every day. This boom, coupled with the affordability and anonymity enjoyed by perpetrators, has also led to cyber tools being deployed in hybrid warfare operations. These are coercive operations blending instruments such as economic pressure, disinformation and military aggression. Thus, increasingly, the cyber discussion has assimilated a military dimension, leading NATO to recognise it in 2016 as a domain of operations subject to its collective defences.

Although, conceptually, cyber defence was initially limited to the protection of military assets, its breadth is widening given that the military sphere, just like the civilian sphere, depends on a safe cyberspace to protect critical infrastructure such as electric grids, water systems, banking, transport, communication systems and, not least, the flow of goods and services. Attacks on critical infrastructure have the potential to: completely paralyse a country – as witnessed during the 2015 attack on Ukraine's power grid, right before Christmas Eve; to disrupt electoral processes – as was revealed during the 2016 US presidential election; and to upset entire sectors with the risk of causing physical damage – exemplified by recurring attacks on Saudi Arabia's oil facilities and companies; not to mention the potentially catastrophic effects of a successful cyber attack on nuclear weapons or facilities. The World Economic Forum (WEF) has rated cyber attacks on critical infrastructure as the fifth top global risk in 2020.

### New technologies in cyber defence: Assets or vulnerabilities?

The seemingly uncontrollable upsurge in disruptive technologies is already creating governance gaps. Increasingly, disruptive technologies enabled by machine-learning and automation are integrated into cyberspace operations such as information warfare, for example. This poses challenges with, on the one hand, the speed and volume of information surpassing governments' and authorities' ability to tackle it, and, on the other, little room for decision-making: by the time attacks are identified, the damage is already done.

For example, what is referred to as *offensive artificial intelligence* (AI) is thought to be able to 'mutate itself' to adapt to its environment and to expertly compromise systems with minimal chance of detection. Such AI-enabled technologies could go as far as to impersonate trusted users, linger undetected in computer systems and learn a user's behaviour, and launch sophisticated attacks that are harder to detect.

While the connectivity of systems logically implies cyber vulnerabilities, digital technologies could be equally deployed to protect assets and even to respond offensively to an attack. The same AI-enabled technologies could also be used *defensively* to rapidly detect such threats and provide better prevention to protect against them.

## Are we at (cyber) war?

Political scientist Joseph S. Nye Jr. argues that 'in the classic duality between war and peace, [cyber attacks usually fall] into a 'gray zone''. The development of digital markets and connected societies goes hand in hand with security and defence challenges. Indeed, digital innovation is ever more subject to geopolitical tensions and rivalries. These aspects are particularly visible in the emerging race for technological breakthroughs between governments and businesses alike – the digital arms race (more in Burning Issues below).

Disruptive technologies are being leveraged to an ever greater extent by both state and non-state actors in the *gray zone* challenging existing norms, laws and institutions, generally operating below the armed conflict threshold. It is becoming more widely understood that strategic competition is being increasingly played out in the digital sphere.

### Two viruses, one answer: coronavirus, cyber and solidarity

The 2020 coronavirus pandemic, in addition to sparking unprecedented health security measures around the globe has also seen a spike in cyber attacks, riding the wave of the virus in the information sphere. It was reported that perpetrators are taking advantage of the millions of people working from unprotected WiFi connections, but also of public fear, tempting them to click on malicious links.

Attackers are therefore capitalising on the confusion and panic surrounding the outbreak. For example, one malicious scheme used an interactive map created by Johns Hopkins University to spread password-stealing malware. Cyber criminals have been disseminating fake emails impersonating national authorities and the World Health Organization. A cyber attack targeting Lithuania falsified the email address of the Lithuanian defence ministry and alleged that the government was trying to hide information about the coronavirus from its citizens. The email had been sent to other European countries and public institutions. Other examples include attacks on Prague Airport and on several Czech hospitals aimed at severely damaging victims' computers.

European Commission President Ursula von der Leyen has warned citizens about the increase in cybercrime since the pandemic took hold. Meanwhile, hospitals are also warned to take precautions given they increasingly represent cyber targets. In this context it is clear that the best response to both the cyber threat and the pandemic is solidarity. Paralysing malware can spread even faster than the coronavirus and wreak havoc in European societies. It is through solidarity, information-sharing and mutual assistance that European countries stand the best chance of defending themselves against both types of threat. All EU institutions have actively spread awareness of these risks while also debunking false narratives circulating across cyberspace. Europol has begun to map the post-coronavirus cyber threat landscape in order to reinforce resilience and proactively engage in prevention.

The WEF placed cyber attacks in their top 10 global risks in terms of both likelihood and impact for 2020. The EU Agency for Cybersecurity (ENISA) demonstrated that the 2018 cyber threat landscape was dominated by ransomware, cryptocurrency and phishing attacks. Cyber threats and risks vary from country to country, depending on the complexities of their respective digital environments.

Cyber offensive actors are increasing in diversity, ranging from lone wolves, to state and non-state actors. Very often non-state actors act as proxies for belligerent states, or both state and non-state actors create false flags for the deceitful attribution of an attack. A Financial Times article finds governments still unable to establish credible collective cyber defence, instead relying on largely 'old-fashioned tools'. The writer goes as far as to say that 'we are at – or very near – war in cyber space today'.

Rather than characterised by isolated attacks, the cyber realm has become something of a battlefield in itself, where the race for cyber superiority has resulted in a security paradox. For example, in its 2015 defence white paper, China named cyberspace as a 'new commanding height' in strategic competition while the US 2018 cyber strategy makes cyberspace responsible for 'altering the strategic balance of power'. Experts argue that China and the US might be the only individual countries financially able to pursue a cyber sovereignty-focused approach.

When asked to cyber-characterise the past decade, experts used words such as 'neglect', 'unexpected consequences', 'covert competition' and 'militarisation'. In contrast, when asked to predict key emerging cyber trends for the next decade, they answered 'cyber hygiene', 'speed' and

'automation' of both protection and of vulnerability discovery. Although research findings generally oscillate between hope and angst, there seems to be international consensus on the need for cyberspace norms to guide the development of trustworthy and secure systems. There is a gap – or an opportunity – for credible leadership in pioneering responsible cyber behaviour governance. Thus, cyber defence and cyber diplomacy are directly linked in addressing cyber threats in a responsible, appropriate and legally-compliant manner.

## Burning issues

**Arms control.** The specialised literature brims with analyses of a new digital/cyber/technological arms race. It is argued that cyberspace 'has become an extension of the military domain', triggering this race. The most active actors in the digital arms race are thought to be rival states and countries either with recent conflict experiences or with active territorial disputes. Recommendations for mitigating the potentially destructive consequences of an arms race include the development of an internationally-agreed moratorium on certain targets, such as civilian facilities, the initiation of arms control security-building measures by the United Nations (UN) and the OSCE, and collaborative approaches to fill the cyber regulatory governance gap.

**Rules of engagement for cyber warfare.** Whether a cyber attack can be considered an armed attack argues Joseph Nye Jr, 'depends on its consequences rather than the instruments used'. This is complicated further by the asymmetric nature of cyber warfare, whereby lone wolves are able to exploit fissures in the defences of large multinational companies and even countries. Although UN initiatives such as the Group of Governmental Experts and the Open-Ended Working Group are essential for 'advancing responsible state behaviour in cyberspace', at the moment there are no globally-agreed international agreements or binding guidelines on rules of engagement.

**Dual use export control regimes.** The 'gray zone' of cyber war also results from the fact that cyber tools can be used for both civilian and military purposes – they are dual-use devices. For example, a single line of coding could make the difference between a program that is weaponised and one that is not. Equally, commercially accessible programs can be used for both legitimate and ill-intended purposes, depending on the user's intention. This makes the export of cyber tools particularly difficult to regulate. For its part, the EU is already considering including cyber-surveillance technologies in its dual-use export control regime.

# EU cyber

According to the Global Cybersecurity Index 2018, regionally, Europe fares best in terms of cyber public awareness campaigns, research and development, and educational programmes, as well as cyber industry and capacity building. Europe recorded more bilateral, multilateral and international agreements than other regions in the world, while also enjoying the highest score for participation in international forums.

Nevertheless, attacks targeting Europe show no sign of slowing down. In 2018 alone multiple attacks suspected to originate from China, Iran, Pakistan or Russia occurred alongside others whose perpetrators remain unknown. Examples range from the attack attributed to the Russian military intelligence service on the Organisation for the Prohibition of Chemical Weapons, to the reports of the hacking of EU diplomatic communications by China's People's Liberation Army.

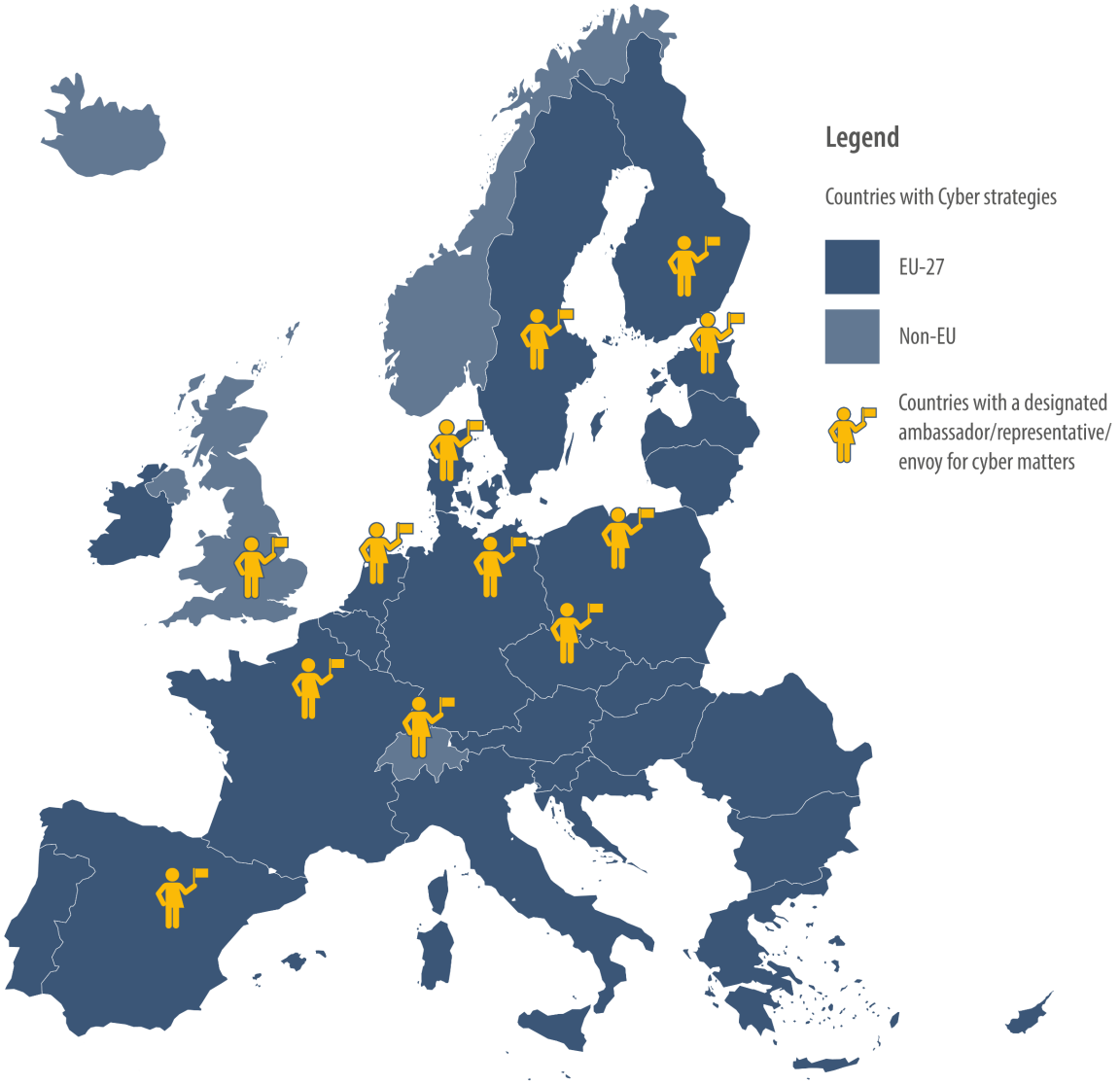
Although the EU's last cybersecurity strategy dates back to 2013, it was revised in the 2017 cybersecurity package and several guiding documents, including the EUGS, have been issued. The strategy makes several key cyber-related points:

- pledging EU support for critical infrastructure protection and cyber crisis management, and for stimulating cooperation between Member States on political, operational and technical cyber issues;
- calling for technological capabilities for cyber resilience to be bolstered across the spectrum;
- proposing the mainstreaming of cyber issues across all EU policy areas; and

- aiming to enhance cyber cooperation with core partners, international organisations and through public-private partnerships.

Recognising the omnipresence of cyber threats, all EU Members have developed cyber strategies – as Figure 1 illustrates. Some have also appointed cyber ambassadors, envoys or representatives, and drafted sub-strategies on cyber defence. It has also been suggested that an EU Special Representative for International Cyberspace Policy should be appointed to 'defend the EU's positions on the international stage'.

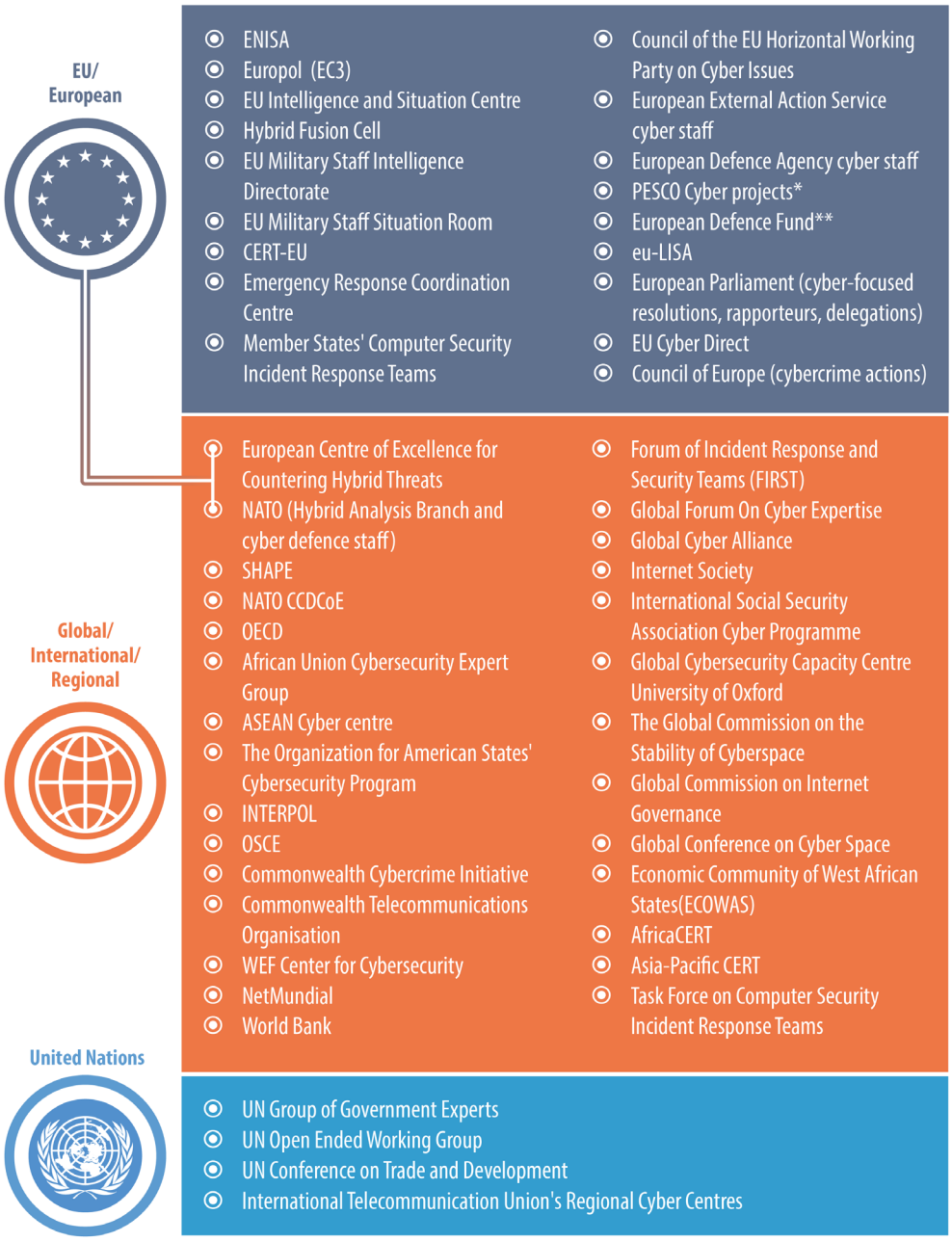
Figure 1 – European countries with cyber strategies and representatives




Source: EPRS, 2020.

The mapping in Figure 2 highlights the key EU and international bodies dealing with cyber. Examples of EU-level cooperation include ENISA's close cooperation with the European Defence Agency (EDA), with the EU Computer Emergency Response Teams (CERT-EU) and with Europol's European Cybercrime Centre (EC3). According to its 2018 report, ENISA also engages with the European Commission's Directorate-General for Communications Networks, Content and Technology and with the European Security and Defence College.

Figure 2 – Non-exhaustive mapping of cyber stakeholders




*Eight projects are cyber-focused while at least 19 others have a cyber component.
**The Fund is also geared towards funding cyber projects, among other priority areas.

Source: EPRS, 2020.

The primacy of international law when it comes to cyberspace, and international relations in general, is a fundamental European principle. This belief is rooted in the EU's efforts to forge a cyber architecture for itself. Besides the above operational bodies, the EU's first cyber legislation – the 2016 Security of Network and Information Systems (NIS) Directive – boosted cybersecurity standards in the EU. The European Commission now intends to review the NIS Directive to 'further strengthen overall cybersecurity in the Union'. In 2017, the Commission adopted the Cybersecurity Act, revamping and bolstering ENISA and establishing an EU-wide certification framework. The package containing the act also includes a blueprint to help EU members and EU institutions respond to cyber incidents by means of existing crisis management mechanisms. Two additional architectural elements followed in 2018, with the Commission proposals to create a network of cybersecurity competence centres and a European cybersecurity industrial, technology and research competence

centre which is supposed to strengthen the EU's cyber capabilities. Since 2010, the EU has also organised bi-annual pan-European cyber exercises (CyberEurope). The 2020 edition will focus on a healthcare cyber attack scenario. Lastly, several specific projects under the umbrella of permanent structured cooperation address cyber issues, such as the cyber rapid response teams and mutual assistance in cyber security project, while many others implicitly entail a cyber dimension.

The EU has ten strategic partnerships.[1] Most of these have a cyber dimension[2] that the EU is working to connect with its broader strategic objectives, including on cyber-diplomacy. For example, a joint statement following a 2015 high-level summit between the EU and South Korea committed the two to 'increase bilateral cooperation on cyberspace' and to 'strengthen the global partnership in response to threats arising from cyberspace'. They also have a cyber policy consultation platform and cooperation between their respective CERTs. Additionally, the EU has cyber engagements with the African Union – their February 2020 joint communique mentions cyber cooperation – and with the Association of Southeast Asian Nations (ASEAN), whose joint statement from August 2019 highlights their intention to strengthen 'cooperation on cyber issues'. Experts argue that cyber partnerships of this kind are becoming an increasingly essential element of the EU's cyber diplomacy goals and action.

Ultimately, the EU's ambition to become more capable, whether 'strategically autonomous' or 'technologically sovereign', also depends on credible cyber defence and diplomacy. The cyber dimension itself is witnessing pushes towards sovereignty by individual powers, considering it a prerequisite for competitiveness. It is nevertheless argued that 'only a long-term cyber diplomacy coordinated at the European level could help to bring about security in Europe and avoid conflict escalation'.

## The EU's cyber diplomacy toolbox

The EU's international cyber engagements, including its response to malicious activities, are conducted under its common foreign and security policy (CFSP) and common security and defence policy (CSDP).

The EU's 2015 Council conclusions on cyber diplomacy call for a 'coherent international cyberspace policy that promotes EU political, economic and strategic interests' through engagement with international partners, industry, academia, and civil society. Overall the conclusions outline a values-based EU approach – from human rights protection and gender equality to freedom of expression – for cyber capacity-building in third countries and cross-sector international engagement with partners and organisations. The conclusions also highlight difficulties in ensuring consistent and meaningful participation of all stakeholders, owing in part to the large number of uncoordinated forums.

In October 2017, EU Member States adopted a cyber diplomacy toolbox.[3] The document is unambiguous about the security benefits of a joint EU diplomatic response to malicious cyber behaviour, highlighting the deterrent effect upon potential aggressors. At the same time, it conditions the effectiveness of this approach upon a 'shared situational awareness agreed among Member States' and proportionality of response. Most importantly, the aim is to set guidelines for malicious cyber activity at all levels of the conflict spectrum:

- preventive measures – cyber confidence and capacity building abroad, awareness raising activities of EU cyber policies;
- cooperative measures – political and thematic dialogues or EU diplomatic démarches;
- stability measures – official statements by EU leadership, Council conclusions, diplomatic engagements in international forums and démarches;
- restrictive measures (sanctions) – travel bans, arms embargos, freezing of assets;
- EU support for Member States' lawful responses should they fall victim to a cyber act: including in the case of invoking the EU's mutual assistance clause, Article 42 (7) TEU and the solidarity clause, Article 222 TFEU. NATO Allies can also invoke Article 5.

The document also refers to the need for 'shared situational awareness', enabled by constant exchanges on the cyber threat landscape and coordination among all relevant EU and national bodies. The Council's Horizontal Working Party on Cyber Issues and the Political and Security Committee are prime candidates for coordinating these practices.

Establishing shared situational awareness is key when it comes to one of the most sensitive aspects of cyber operations: attribution. While the EU toolbox naturally emphasises that each Member State is free to take a sovereign political decision with respect to the attribution of offensive cyber activities, it also notes that for a joint EU response to be effective, collective assessment and action are necessary. Coordination of action with 'like-minded partners and international organisations' is also envisaged. Some analysts have interpreted the EU's cyber diplomacy action as its intention to position itself as 'a force for peace'.

Directly contributing to the EU's cyber diplomacy goals is the EU Cyber Direct project. Financed through the EU's Partnership Instrument, the project aims to develop dialogues with the EU's strategic partners. It also aims to become a platform where governmental and non-governmental actors discuss cyber norms, responsible cyber behaviours and confidence-building measures.

### The future EU-UK cyber relationship

The UK is a leading nation in terms of its cyber defence and security arsenal. It enjoys a strong state apparatus in support of its cyber policy, and is in the process of creating a National Cyber Force to complement the existing National Cyber Security Centre. The International Telecommunication Union's Global Cybersecurity Index 2018 ranks the UK top in terms of legal and organisational preparedness for cyber threats.

Having now left the Union, the UK has become a third country to the EU, including as regards cyber policy. As threats pay no heed to a country's affiliations, and great power competition is showing no sign of abating, strong EU-UK cyber cooperation is highly desirable. The British government's 2017 policy paper on the future foreign policy relationship recognises cyber threats as common challenges, acknowledging that the two 'operate in a single cyberspace'. The paper supports close cooperation on cyber threats to promote stability in cyberspace and international standards.

The final political declaration provides room for cyber cooperation as part of a broad security partnership, encourages cooperation 'to promote effective global practices' and confirms the establishment of a bilateral cyber dialogue. Recent policy documents drafted by the government led by Prime Minister Boris Johnson make no mention of any security and defence cooperation, nor of cyber matters. In contrast, the latest negotiation guidelines (March 2020) from the European Commission include a thematic cyber chapter. The section provides for a regular cyber dialogue, sharing of best practices, cooperation on cyber norms and regional cyber confidence building. It also specifies coordinating diplomatic responses and engaging in joint exercises. The EU's position envisions 'voluntary, timely and reciprocal' cooperation between CERT-EU and the UK's CERT and, upon invitation, UK participation in various ENISA activities.[1] A broader chapter on the security partnership was published separately from the document, following the UK's wish to exclude these themes from the current negotiations, but it excludes cyber.

EU cyber diplomacy actions have global reach. CyberEast (in cooperation with the Council of Europe) and EU4Digital are examples of concrete cooperation with the Eastern Partnership countries – Ukraine, Moldova, Belarus, Georgia, Armenia and Azerbaijan. In West Africa, the OCWAR-C project aims to enhance regional cybersecurity, and in Southeast Asia, the YAKSHA project aims to build cyber partnerships. There are many more such projects.

Lastly, the EU is engaged or present in some capacity in a large number of multilateral cyber initiatives and forums. The EU's own positions are guided by principles developed in a UN context, in accordance with international law. The cyber diplomacy toolbox conclusions themselves take into account the guidelines from the UN Groups of Governmental Experts (GGE). The EU is thus committing itself to actively support 'the development of voluntary, non-binding norms of responsible State behaviour in cyberspace and the regional confidence building measures' in which the OSCE is leading the work. The EU has also applied its cyber diplomacy principles to the G20 forum and the Paris call for Trust and Security in Cyberspace, for example.

# Transatlantic cyber

## Bilateral EU-US cooperation

The US has a longstanding history of security and defence cooperation with European countries and with the EU. Despite having taken different domestic approaches to cybersecurity, the two sides of Atlantic generally recognise the value of cooperation with likeminded partners for cyber hygiene, prevention and responsible behaviour. Of the EU's cyber partnerships, the one with the US is 'by far the oldest and most developed', going back to the early 2000s.

The cooperation itself takes place in various formats. One is the Working Group on Cyber-security and Cyber-crime, established in 2010. Its first joint cyber exercise took place in 2011. A high-level EU-US strategic cyber dialogue began in 2014 to formalise cooperation on human rights in cyberspace, cyber norms, confidence- and capacity-building, and the application of international law. During the third edition of their cyber dialogue the two partners launched the Transatlantic Cyber Policy Research Initiative to increase the research capacity on cyber issues. The fifth and latest meeting under the EU-US cyber dialogue occurred in 2018. The two also liaise through an Information Society Dialogue which focuses on internet governance.

Moreover, the two sides also exchange information on the basis of a NATO technical agreement and as signatories of the Council of Europe Convention on Cybercrime, also known as the Budapest Convention. Through its Horizon 2020 programme, the EU has awarded funding for project AEGIS, supporting the EU-US cybersecurity and privacy dialogue. Their active participation in multilateral fora such as the UN GGE, the OSCE, the Organisation for Economic Co-operation and Development (OECD) and also the G7 and G20 formats, also enables the US and the EU (institutions and Member States) to collaborate on cyber matters.

Notwithstanding a fruitful recent history of cyber cooperation, it is argued that a 'certain degree of distrust' has been overshadowing the relationship since the revelations of whistle-blower Edward Snowden. Despite commitments in the 2018 US Cyber Deterrence strategy to 'actively participate in global efforts' to uphold openness, freedom and innovation, bilateral cyber dialogues have not been held since 2018. In May 2019, President Trump declared a national cyber emergency, following a trend of national securitisation of ICT trade and technology transfers. A specialised study urges the US national security community to closely cooperate with its allies and partners to jointly uphold an open internet and free flow of ideas against pressure from authoritarian regimes. It recommends 'fusing offensive cyber infrastructure' to advance towards achieving a common cyber threat assessment and interoperability. Others urge both sides to honour the longstanding transatlantic cooperation on cyber threats by creating 'a collective defence shield against our common opponents in this new domain of cyberwarfare'.

## NATO

The Atlantic Alliance has recognised cyberspace as an operational domain since 2016. This means that cyber attacks can be categorised as a form of warfare and therefore trigger NATO's mutual defence clause – Article 5. In July 2016 it also released a Cyber Defence Pledge, committing each Allied country to enhance their national infrastructures and networks following the principle that 'we are only as strong as our weakest link'. The pledge acknowledges the contribution brought by the EU-NATO partnership to cybersecurity and defence, and commits to reinforcing it. At the 2018 Brussels Summit, Allies expressed determination to use their 'full range' of cyber capabilities to 'deter, defend against, and to counter the full spectrum of cyber threats'.

The Alliance itself has taken measures to beef up its cyber capabilities by creating cyber rapid reaction teams that are constantly on standby, it has included a Cyber Operations Centre as part of its command structure and has taken steps to strengthen industrial cooperation through the NATO industry cyber partnership. Most recently, in February 2019 it drafted guidelines for responding to cyber threats.

Since the 2016 Warsaw Summit, EU-NATO cooperation has thrived and expanded across multiple fields, including cyber. Work is ongoing to improve information-sharing and promote training by means of joint cyber exercises, such as the parallel and coordinated exercises (PACE). The latest edition of NATO's flagship Cyber Coalition exercise took place in Estonia in 2019. As mentioned above, the EU and NATO have also been cooperating by means of a Technical Arrangement on Cyber Defence since February 2016, which, among other things, provides for cooperation between CERT-EU and the NATO Computer Incident Response Capability. In addition to cooperation between NATO and EU staff, the relationship is also strengthened through diplomatic fora such as the NATO Parliamentary Assembly – where the European Parliament also participates – and through coordination between the EU's Hybrid Fusion Cell and NATO's Hybrid Analysis Branch. Equally valuable are the EU-NATO Centre of Excellence for Countering Hybrid Threats, the NATO CCDCoE, the NATO School in Oberammergau, Germany, and the NATO Defence College in Rome, Italy.

## Global and European cyber

Demands for more coherent international action and cooperation on cyber issues have been made time and again by a wide array of stakeholders. The urgent need for international cyber statecraft has become increasingly obvious with the fast-paced technological developments occurring worldwide. The international cyber policy realm is blessed with a multitude of initiatives but at the same time cursed by their fragmentation.

The most prominent multilateral cyber diplomatic action is undertaken through the work of the UN Group of Government Experts, whose findings – promoted by the EU – proved decisive for the global consensus on the applicability of international law to cyberspace. Important work is ongoing through governmental alliances, public-private partnerships, academic consortia and mixed expert commissions. Examples include the Global Commission on the Stability of Cyberspace – focused on cyber norms and responsible cyberspace behaviour; Microsoft's proposed Digital Geneva Convention – proposing a cross-sector legally binding agreement; Siemens' and the Munich Security Conference's Charter of Trust initiative – aiming to set general standards for cybersecurity; or French President Macron's Paris Call for Trust and Security in Cyberspace – a non-binding initiative to establish common international cyber norms. Despite the fragmented plethora of initiatives (as Figure 2 also illustrates), some experts remain optimistic about the deepening multi-stakeholder commitments for developing and upholding an open, safe and principled cyberspace.

The EU and its Member States are actively promoting various of these initiatives in different forms. For example, the EU's cybersecurity act included a commitment to protecting the 'public core' of the internet, a norm developed by the Global Commission on the Stability of Cyberspace.

## European Parliament views

The European Parliament has consistently advocated robust EU-level cyber measures. In a June 2018 resolution focused on cyber defence, Parliament confirmed its commitment to an open, free and secure cyberspace, upholding EU values, while calling upon EU Member States to implement the EU's approach to cyber diplomacy and cooperate with NATO in formulating criteria and definitions for cyber operations. It consequently welcomed the EU's cyber diplomacy toolbox and called for a proactive, cross-sectional foreign policy approach to strengthen it. In March 2019, Parliament approved the cybersecurity act, establishing the first EU cyber-certification scheme and giving ENISA a permanent mandate. In January 2020, Parliament called for increased EU efforts to confront cyber threats, deeming the active cooperation between the EU and NATO to be vital. Lastly, Parliament recalled that cyber attacks 'could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union)'.

## MAIN REFERENCES

Bendiek A., The EU as a Force for Peace in International Cyber Diplomacy, Stiftung Wissenschaft und Politik, April 2018.

Renard T., 'EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain', *European Politics and Society*, January 2018.

Nye Jr S. J., 'Deterrence and Dissuasion in Cyberspace', *International Security*, Vol. 41, 2017.

## ENDNOTES

[1] With Brazil, Canada, China, India, Japan, Mexico, Russia, South Africa, South Korea and the United States.

[2] These take the form of formal bilateral dialogues, technical expert meetings or working groups.

[3] The formal title being 'Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities'.

## DISCLAIMER AND COPYRIGHT



eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)