EUROPEAN POLICY CENTRE

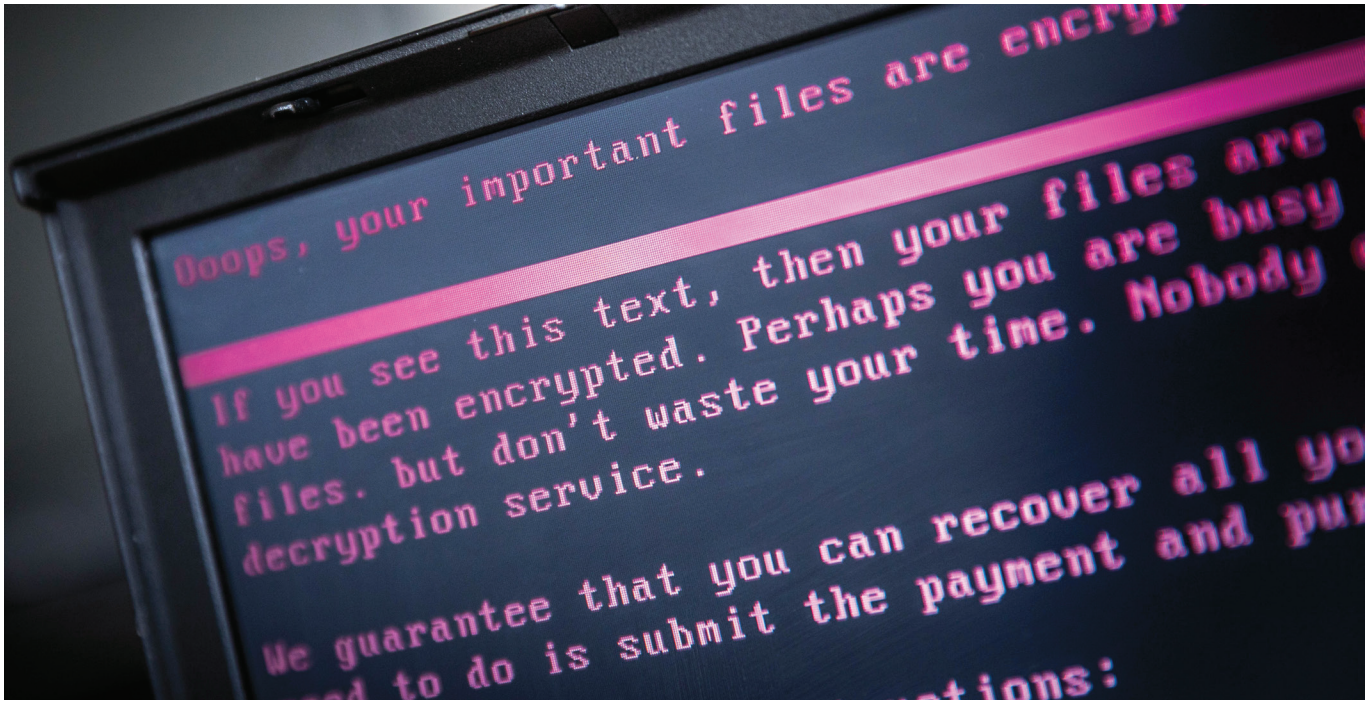
DISCUSSION PAPER

EUROPE IN THE WORLD PROGRAMME

18 MARCH 2019

Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox

Paul Ivan



Credit: Rob Engelaar/ANP/AFP

Table of contents

ABOUT THE AUTHOR

Paul Ivan
Senior Policy Analyst
European in the World programme

DISCLAIMER

Executive summary

Malicious cyber activities have become a growing threat, a fact that has become more visible in recent years through several massive cyberattacks. While the European Union (EU) has been active in the field of cybersecurity for a number of years, it has not yet put in place diplomatic tools to respond to cyberattacks, nor has it attributed cyberattacks. However, EU member states have made progress in the development of a cyber diplomacy toolbox containing a number of measures, from preventive ones to the use of sanctions. This work needs to be finalised, so that the Union's toolbox can become operational and used when needed.

This paper analyses the newly created framework for the EU's diplomatic response to malicious cyber activities, the challenges that hamper a unified EU response and possible ways to address these challenges. It focuses on issues linked to the attribution of cyberattacks and on the most powerful diplomatic instrument to be adopted to respond to them: the use of cyber sanctions.

The attribution of cyberattacks poses a number of challenges, both technical and political. Many member states lack the required cyber and intelligence capabilities, and the political and administrative processes necessary to properly attribute cyberattacks. Moreover, attribution remains a political decision for national leaders to take and, like most foreign policy decisions, one influenced by diverse (geo)political considerations. To overcome problems of collective action and achieve unanimity in the EU Council on a common diplomatic response, EU member states and EU institutions should do more to develop common threat assessments and a shared culture of attribution of cyberattacks. For this, member states will need to upgrade their information sharing but also exercise the Cyber Diplomacy Toolbox.

One of the key enablers for collective diplomatic action at EU level will be the necessary strengthening of cyber capabilities, both defensive and offensive. This will require investment in human and technical capacities, but also in creating and updating internal procedures so that the work of cybersecurity professionals feeds into the political decision-making process. While achieving unanimous agreements on attributing cyberattacks to non-EU countries will continue to be challenging, EU countries will still be able to use most of the framework's tools. The most powerful ones, such as the public attribution of attacks or the use of sanctions will have to be wielded carefully, based on strong compelling evidence.

Cooperation with the private sector and with international partners should be pursued. The EU will need to set up an enhanced cybersecurity cooperation with post-Brexit Britain and further develop EU-NATO cooperation in this field. Continued investment in confidence building measures, in the development of norms at the UN level and in global, regional and bilateral cyber dialogues will be crucial to limit some of the alarming developments occurring in cyberspace.

While attributing attacks or adopting sanctions can potentially worsen relations with the particular country concerned, not reacting to cyberattacks is likely to encourage similar or even more damaging behaviour. The EU's cyber diplomacy toolbox, with its attribution and sanctioning tools, is intended to play a role in the calculations of potential aggressors, acting as a deterrent against bad behaviour.

While the cyber diplomacy toolbox is complementary to actions by individual member states, acting together would allow EU member states to be more credible and send a stronger deterrent message. By responding to cyber threats as a united actor, EU countries will be better placed to defend their security, their political and economic interests and further enhance the Union's credibility as an international actor.

Introduction: The warnings have become reality

Hospitals cancel operations, factories temporarily shut down, global companies are put offline, incurring huge losses – the growing risks posed by malicious cyber activities have become an unwelcome reality. The increasing number of cyber incidents has shown that different international actors continue to deploy malicious cyberattacks that can spread rapidly across borders, even beyond their intended targets, compromising ICT systems and causing significant damage. It is also evident that despite the international conversations on cybersecurity taking place at the UN, G20 or in regional formats, **several states continue to employ cyberattacks against various entities in the European Union (EU)**.

Malicious cyber tools have been used by states for well over three decades. The 2007 cyberattacks on Estonia amid Tallinn's disagreement with Russia about the relocation of a Soviet-era statue drew particular attention to this security challenge. More recently, Ukraine has also suffered a series of cyberattacks, including on its electricity grid, which temporarily disrupted electricity supply in 2015 and 2016.[1]

While cybersecurity incidents are a daily occurrence, two massive cyberattacks that spread at a global level and affected several EU member states in 2017 demonstrated the extent of the damage that malicious cyber activities

can inflict. In May 2017, the WannaCry ransomware attack quickly spread around the world, encrypting data and demanding ransom payments in the cryptocurrency Bitcoin. The attack was estimated to have affected more than 300,000 computers across 150 countries[2], causing between USD 4 to 8 billion worth of damages.[3] Among others, carmakers Renault, Nissan and Honda were affected by the attack and were forced to reduce or even stop production at a number of sites in France, the United Kingdom (UK), Romania, Slovenia, Japan, and India.[4] The attack also hit the national healthcare system in the UK, which left hospitals and doctors unable to access patient data and led to the cancellation of operations and medical appointments.[5]

In June 2017, the major NotPetya cyberattack spread from its target, Ukraine, to the rest of the world, affecting numerous companies in Europe. The attack severely affected the Danish company A.P. Møller-Mærsk, the world's largest container shipping company, which saw a large part of its IT infrastructure taken offline, creating a loss of USD 200-300 million.[6] Losses of similar size were registered by the pharmaceutical company Merck & Co., one of the largest in the world, which had to shut down production of one of its paediatric vaccines.[7] According to a White House assessment, the **NotPetya cyberattack created damages amounting to more than USD 10 billion**.[8]

Major attacks such as WannaCry and NotPetya showcased the potential destructive magnitude of malicious cyberattacks, which can have real-life consequences for people and infrastructures. The attacks also highlighted that advanced and digitalised economies are vulnerable to sophisticated attacks that can spread in a matter of minutes. Moreover, these widespread attacks highlighted the need for EU member states to act together to respond to and deter similar attacks.

This paper analyses the development of the framework for the EU's diplomatic response to malicious cyber activities, the challenges that hamper a unified EU response and possible ways to address these challenges. It focuses on issues linked to the attribution of cyberattacks and on the most powerful new diplomatic instrument to be adopted to respond to them, the use of cyber sanctions. Though a very important topic on its own, the paper does not cover the topic of digitally-enabled disinformation.

Major attacks such as WannaCry and NotPetya showcased the potential destructive magnitude of malicious cyberattacks, which can have real-life consequences for people and infrastructures.

The paper argues that EU member states and EU institutions should do more to develop common threat assessments and a common culture of attribution of cyberattacks. They should upgrade their cyber capabilities and learn to exchange information and cooperate better. Member states should invest in all the available tools in the toolbox and employ the more powerful ones based on solid proof and assessments. While member states can continue to face and respond to these threats separately, they are likely to achieve better results working together. Failure to react credibly to future cyberattacks is likely to encourage similar or even more damaging behaviour.

1. The EU response: First steps

Recognising the reality of the threat, the EU and its member states have worked over the past few years to strengthen cybersecurity in Europe and tackle cyberattacks against infrastructures, cyber-espionage, intellectual property theft, and hybrid threats using cyber means. The Union has primarily invested in increased prevention, early warning mechanisms, resilience and coordination.

The 2013 EU Cybersecurity Strategy, the 2016 Network and Information Security (NIS) Directive and the 2016 Joint Framework on countering hybrid threats are major milestones. The NIS Directive, for example, required member states to be equipped to boost the overall level of cybersecurity in the EU by setting up national Computer Security Incident Response Teams (CSIRTs) and a competent national NIS authority. To facilitate strategic cooperation and exchange of information, it also established the NIS Cooperation Group, composed of member state representatives, the European Commission and the EU's Agency for Network and Information Security (ENISA) and the CSIRTs Network, dedicated to sharing information about ongoing threats and cooperating on cybersecurity incidents.

Over the years, the EU has also dedicated resources to cyber diplomacy, both at the multilateral level and through bilateral relations. Since the early 1990s, the EU has been involved in the international debates on internet governance. The 2013 EU Cybersecurity Strategy has been a major step in the development of EU cyber diplomacy, placing the establishment of a "coherent international cyberspace policy for the EU" among its five priorities. Over the years, the EU has also developed cyber dialogues with partner countries, the EU-US partnership (now called the EU-U.S. Cyber Dialogue) being the most developed.

More recently, in 2017, the European Commission proposed a wide-ranging cybersecurity package to

further improve EU cyber resilience, deterrence and response. In December 2018, the European Parliament, the Council and the Commission reached a political agreement on the Cybersecurity Act, which aims to introduce an EU-wide cybersecurity certification and to consolidate the European Union Agency for Network and Information Security (ENISA). As part of the same cybersecurity package, the Commission also proposed the creation of a network of Cybersecurity Competence Centres, a Cybersecurity Competence Community and a new European Cybersecurity Industrial, Technology and Research Competence Centre. The EU is also developing procedures to achieve a coordinated response to large-scale cybersecurity incidents and crises.[9]

The increasing number and gravity of state-sponsored cyberattacks has also increased the political prominence of the challenge. While the EU has been dealing with cybersecurity for a number of years, steps to develop a joint EU diplomatic response to malicious cyber operations have only gained traction at the political level over the last three years. As illustrated below, some EU member states have in recent years attributed cyberattacks, publicly or not.[10] However, the EU as such has generally not attributed cyberattacks and has not taken measures against the state and non-state actors which have been identified as the perpetrators of some of these attacks.

The EU as such has generally not attributed cyberattacks and has not taken measures against the state and non-state actors which have been identified as the perpetrators of some of these attacks.

During its 2016 Presidency of the EU Council, the Netherlands put forward a non-paper on "Developing a joint EU diplomatic response against coercive cyber operations."[11] The document argues **that to influence the behaviour of potential aggressors and thus to reinforce the EU's security it is necessary to clearly signal the consequences of malicious activities**. The document also presents the main principles of the toolbox to be developed, among them the proposal that the EU response should "be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity".

The work on the topic continued and, in June 2017, the EU Foreign Affairs Council endorsed the main principles of a framework for a joint EU diplomatic response to malicious cyber activities – the so-called Cyber Diplomacy Toolbox.[12] The Council conclusions mention a series of possible measures within the framework of the Common Foreign and Security Policy (CFSP) that the EU institutions and member states could undertake, including the use of the most powerful tool – restrictive measures (sanctions). In October 2017, the framework was worked out in more detail with the adoption of a document containing implementing guidelines.[13]

The measures of the EU Cyber Diplomacy Toolbox:

- preventive measures, including confidence-building measures, awareness raising on EU policies, EU cyber capacity building in third countries;
- cooperative measures, including the use of political and thematic dialogues and démarches;
- stability measures, including statements by the EU High Representative and on behalf of the Council of the EU, EU Council conclusions, diplomatic démarches, signalling through EU-led political and thematic dialogues;
- restrictive measures (sanctions); and
- possible EU support to member states' lawful responses.

From a legal point of view, EU member states uphold the international consensus that existing international law is applicable to cyberspace and base their work on the Cyber Diplomacy Toolbox on the existing international legislation and the principles agreed in the reports of the United Nations Groups of Governmental Experts (UN GGE).[14] The 2015 UNGEE report offered a non-exhaustive list of the principles of international law that states must observe in their use of information and communications technologies. Among them are "State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States", as well as the respect and protection of human rights and fundamental freedoms.[15]

The Cyber Diplomacy Toolbox is seen as complementary to the existing EU cyber diplomacy engagement. The implementing guidelines document is a step forward but does not in itself solve some of the challenges to reaching a common EU position, notably on the key issues of attribution and the use of sanctions.

2. Attributing cyberattacks: A continuous challenge

In 2018, the UK and Denmark, together with the United States (US) and Australia, publicly attributed the NotPetya cyberattack to the Russian government[16], while Canada stated that "actors in Russia" were responsible.[17] New Zealand, Norway, Lithuania, Estonia, Latvia, Sweden, and Finland issued statements of support. **Though several EU countries attributed this particularly destructive attack and the EU had already adopted its Cyber Diplomacy Toolbox decision and the accompanying implementing**

guidelines, the EU Council as a whole did not reach an agreement on a collective attribution. The April 2018 Council conclusions on malicious cyber activities only condemned "the malicious use of information and communications technologies (ICTs), including in Wannacry and NotPetya [...]", without attributing the attacks. While the EU member states failed to take collective measures against the actors behind these attacks, the attacks themselves put pressure on the EU to develop a functioning cyber diplomacy toolbox.

While the EU member states failed to take collective measures against the actors behind these attacks, the attacks themselves put pressure on the EU to develop a functioning cyber diplomacy toolbox.

New urgency was added by the hostile cyberattack carried out against the Organisation for the Prohibition of Chemical Weapons (OPCW), which was condemned by the October 2018 European Council. EU leaders also called for measures to "combat cyber and cyber-enabled illegal and malicious activities and build strong cybersecurity" and to "work on the capacity to respond to and deter cyberattacks through EU restrictive measures".[18] Moreover, the President of the European Council, Donald Tusk, Commission President Jean-Claude Juncker and High Representative Federica Mogherini issued a joint statement "on Russian cyberattacks", condemning the "hostile cyber operation carried out by the Russian military intelligence service (GRU)."[19] These events and reactions added additional pressure on the institutions to advance in the operationalisation of the toolbox.

The EU Council's Horizontal Working Party on Cyber Issues (HWP), where EU member states' representatives meet, is currently working on the cyber sanctions regime, the issue of attribution and the strategic communication to be deployed in case of malicious cyber incidents. Among these issues, attribution is probably the most difficult.

According to the implementing guidelines of the toolbox, "attribution could be established, based on an analysis of technical data and all-source intelligence, including on the possible interests of the aggressor". Clearly, the issue of attribution is a complex one, influenced both by technical factors but also by (geo)political and economic ones. While the identification of the source of an attack poses certain technical challenges, it is feasible, as demonstrated by the various attributions already made. However, the political decision to attribute an attack to a specific country or branch of government and, even more, agreeing on a common diplomatic response, will likely continue to prove challenging for a body of 28/27 countries. Some of the challenges that make a collective EU attribution difficult are specific to the cybersecurity sector while others, such as the requirement of unanimity, characterise EU foreign policy more generally.

While some cyberattacks are massive, many of them affect only some individuals or institutions. Getting a full picture of the impact is not always easy. The private sector is strongly impacted by malicious cyber activities but for commercial and reputational reasons, companies are often reluctant to publicise cyberattacks or to (fully) report incidents and losses, which means that valuable evidence and intelligence about threats and offenders is lost. Because the effects of cyberattacks are spread out over a large area and different jurisdictions, this can also lead to a reduced understanding of their full impact and thus to a lack of a shared cybersecurity situational awareness.

Moreover, **only some member states have the cyber and intelligence capabilities and the political and administrative processes necessary to properly attribute cyberattacks**. At different levels, these capabilities are to be found especially in the big member states such as the UK, France, and Germany but also in countries such as the Netherlands, Sweden, Denmark, Finland, and some CEE countries.[20] Advanced cyber capabilities are especially necessary when dealing with sophisticated adversaries, such as the advanced persistent threat (APT) groups.

While the identification of the source of an attack poses certain technical challenges, it is feasible. The political decision to attribute an attack to a specific country or branch of government and, even more, agreeing on a common diplomatic response, will likely continue to prove challenging.

These groups, which have traditionally been associated with nation-state sponsorship, gain unauthorised access to a network and remain undetected for an extended period, posing some of the most serious cyber threats to the EU. The technical staff of the national intelligence services and the national CERTs (Computer Emergency Response Teams), which have followed their activities for years, are familiar with most of these groups' digital signatures and indicators. Although some of the evidence is classified, much of it is publically available in open source, for example in detailed reports produced by private cybersecurity companies. Thus, **while specialists are generally aware of the origin of many of the attacks, the main challenges regarding attribution emerge at the political level, concerning the question of public attribution.**[21]

As mentioned, **while the EU as whole has generally not attributed cyberattacks, some member states have**. The UK has some of the best capabilities in this field and

has been more willing to attribute cyberattacks. In October and December 2017, the UK and the US governments publicly attributed the massive WannaCry cyberattack to North Korea and its government-sponsored hacking group known as the Lazarus Group.[22] In December 2018, the UK, the US and a number of other countries held elements of the Chinese government responsible for an extended malicious cyber campaign targeting intellectual property and sensitive commercial data in Europe, Asia and the US.[23] This was the first time that the UK government publicly named elements of the Chinese government as being responsible for a cyber campaign.

If the EU is just starting to address government-sponsored cyberattacks, the US, benefiting from a less fragmented decision-making system and better equipped cyber agencies, have been more active both in bringing criminal charges against government-sponsored hackers and in putting in place sanctions against them and their organisations. In September 2018, the US Department of Justice formally charged a North Korean programmer for several cyberattacks, including for his role in the creation and spread of the WannaCry attack.[24] In October 2018, the US Department of Justice announced criminal charges against seven Russian military officers for several hacking operations. These included the hacking of various sporting and anti-doping organisations, a US nuclear power company, the Netherlands-based OPCW and the Switzerland-based Spiez Laboratory. Both the laboratory and the OPCW were investigating the poisoning of a former Russian agent in Salisbury in the UK.

3. Challenges regarding collective action

One reason why the EU 27/28 struggle to take collective action is the fact that the Union's decision-making process on foreign policy matters is cumbersome, requiring the unanimous decision of all EU governments. This is a high threshold that is often not easy to overcome, especially when decisions concern third countries with which some member states have strong links or interests.

One reason why the EU 27/28 struggle to take collective action is the fact that the Union's decision-making process on foreign policy matters is cumbersome, requiring the unanimous decision of all EU governments.

Having the technical and institutional capacity to attribute cyberattacks does not necessarily translate into the political will to ask for the support of EU partners and push for a common reaction. Big member states with advanced cyber capabilities also have complex international interests, which may require a delicate balancing act in relation to third countries. Sometimes, these member states may not be willing to deal with malicious cyber activities originating from third countries through the EU framework, sometimes counting to solve or leverage the issue on a bilateral basis.

While the Cyber Diplomacy Toolbox does not preclude action by individual member states, **national initiatives are not always effective**, even in the case of big member states. For example, although the UK has repeatedly approached China on this topic, it continued to be confronted with sophisticated malicious cyber activities originating in the Middle Kingdom.[25] Bilateral dialogues on cyber issues between several EU member states and Russia also don't seem to advance.

The EU member states also display different situational awareness and threat assessments in this field. This is due to, among other factors, the different levels of digitalisation of member states' economies, the different scale of their cyber vulnerabilities, their different cyber capabilities and different political, security and economic priorities and interests. Moreover, most cyberattacks affect member states to different degrees, which results in different assessments of their gravity, a lack of a shared security perception, and raises issues regarding solidarity with a view to a common response.

EU member states also display different situational awareness and threat assessments in this field.

On top of that, for a variety of reasons such as national security concerns, and a lack of sufficient trust and professional practice, **member states' intelligence agencies are also often reluctant to share classified information with all their EU counterparts**. Since attributing a cyberattack to a third party or country can entail negative political or economic consequences, many countries are reluctant to agree to strong common measures based only on trust and incomplete information.[26] Moreover, making a wrong attribution would have costs in terms of credibility. Among the big member states, Italy is the one mostly calling for caution in dealing with this issue.[27] At the other end of the spectrum, Denmark and the United Kingdom have been publicly attributing cyberattacks and are pushing for a more ambitious EU policy.

4. Cyber sanctions: Tools to change behaviour

The issue of attribution is likely to remain a difficult one. However, the question of the use of sanctions also raises a range of problems. **The EU will be able to adopt individual sanctions against perpetrators of a cyberattack without attributing that particular cyberattack to a state.** At the same time, establishing a new sanctions regime and imposing sanctions for actions in a domain in which some definitions and international law are not well-established will require careful consideration. **The proof supporting a sanction listing will need to be solid and able to withstand a challenge in court, while the goals of the sanctions should be clear.**[28]

The implementing guidelines document mentions that restrictive measures could be used by the EU against a state that carries malicious cyber activity or is "responsible for the actions of a non-state actor that is acting under its direction or control". However, the types of sanctions being discussed so far in the Council only target individuals or entities, not countries. The member states will have to clarify the scope of the sanctioning regime.

An October 2018 non-paper[29] on cyber restrictive measures put forward by Denmark, Estonia, Finland, Lithuania, Latvia, the Netherlands, Romania, and the UK called for the urgent need to implement a sanctions regime to address malicious cyber activities. According to the document, the new sanctions regime is needed to change behaviour and to "strengthen the consensus around responsible state behaviour" by imposing consequences on criminal actors who are, in practice, beyond law enforcement. The change in behaviour can be achieved by signalling that malicious cyber activity has consequences, by constraining decision-makers who might consider using malicious cyber tools (for example by blocking their access to financial resources) or through coercion by imposing other meaningful consequences. The balance between the different sanctions' goals (to coerce, constrain or signal) will differ from case to case.

The currently debated EU cyber sanctions regime would follow on the recently approved EU sanctions regime addressing the use and proliferation of chemical weapons.[30] However, the cyber sanctions will pose more complex challenges given that definitions and legislation about what is acceptable and what should be 'sanctionable' behaviour are not as well established at the global level as in the case of the use of chemical weapons. Importantly, **intelligence gathering will likely be excluded from the listing criteria**, as there is no international treaty regulating cyber espionage in peacetime, or espionage for that matter. Among others, this would mean that that the member states and the companies affected will need to deal with the critical problem of industrial espionage through other means.

EU will be able to implement sanctions even without the collective EU attribution of an attack to a specific country.

The adoption of cyber sanctions also raises legal concerns linked to the level of proof needed to compellingly attribute an attack and support a sanctioning decision. In recent years, due to insufficient evidence, the EU Council has lost several cases regarding sanctions listings in front of the European Court of Justice. This adds to the caution of some member states regarding a cyber sanctions regime. It also demands that **any decision on sanctions will need to be based on convincing evidence, able to withstand a case in court**.

At the same time, the EU will be able to implement sanctions even without the collective EU attribution of an attack to a specific country. The October 2018 non-paper mentions that any decision to impose cyber sanctions would not be dependent on "the public attribution of cyber operations which is a separate, sovereign political decision taken by member states". Of course, if the individuals or entities identified as the source of a cyberattack have strong links to the state structures of a non-EU country, avoiding public attribution to that particular country would be difficult.

5. Operationalising the Cyber Diplomacy Toolbox

EU member states will have to agree on the details of the new sanctions regime and the operationalisation of the toolbox. While the EU cyber sanctions regime is likely to be agreed upon soon[31], the more difficult issue of attribution will likely remain a challenge.

To put the toolbox into practice and improve their cybersecurity, member states will have to take a series of measures. This involve the strengthening of their cyber capabilities, raising awareness among the public and decision-makers but also creating and upgrading their internal governmental processes to better inform decisions. If they are to adopt common decisions in this area, member states need to work towards common threat assessments and a common culture of attribution. For this, **improving the sharing of information is**

fundamental. Working with the private sector and with international partners will also be key. The following sections will dwell into these issues and provide a set of recommendations.

Strengthening cyber capabilities

Many EU countries need to improve their cyber capabilities, including in cyber forensics[32], in order to improve their situational awareness, their ability to respond to and recover from attacks, and their capacity to attribute cyberattacks. Strengthening the cyber capacity of member states is one of the key enablers of collective diplomatic action at EU level. This involves investment in both human and technical capabilities. More investment into the training of cybersecurity specialists and their hiring and retention in public service is needed across the Union. Part of the EU funds for cybersecurity should also be used in the EU member states that are lagging behind.

Strengthening the cyber capacity of member states is one of the key enablers of collective diplomatic action at EU level.

Too often, cyber intrusions or the placement of malicious software in politically or commercially sensitive EU networks are discovered very late. Improving detection capabilities also involves investing in different technical capabilities, including the placement of sensors and digital beacons in relevant locations on the internet. To improve their defence mechanisms, EU member states should also increase their investment in cyber offensive capabilities as "it is very hard to do defence if you have no experience with offense."[33] This would be in line with developments in other parts of the world, including with allies such as the US[34] or Australia[35] which are moving towards more robust cyber defences and "forward cyber defence".[36] The EU should avoid trailing behind.

Raise awareness and update internal processes

As the number and the impact of various types of malicious cyber activities has increased, so has the awareness of the public and of decision-makers. However, much more needs to be done to educate the general public, the private sector, the public administrations but also decision-makers, who in many cases have a very weak grasp of the subject.

Besides the necessary human and technical capabilities, **member states should also adopt and update their internal procedures so that the work of technical specialists feeds into the decision-making process and into political decisions**. Given the potential impact of cyberattacks, the issue should not be only left to a limited number of specialists who understand the topic and to working-level bureaucrats.

Often, the political attention span dedicated to this topic tends to be short lived. While a cyberattack can lead to calls for decision-makers to take action, achieving attribution and gathering sufficient evidence usually takes time. Experience has shown that during this time, the issue is likely to drop from the political radar. Thus, following through after an attack, maintaining attention and allocating adequate resources to identify the source of the attack is key.

Appropriate measures and common diplomatic messages

When significant malicious cyber activities are identified, EU member states should consider the appropriate measures to be taken. **Reaction to a cyberattack does not require certainty or near certainty regarding the origin of an attack, and many of the measures in the toolbox do not require attribution.** Additionally, the choice of the measures to be taken will need to be tailored to the degree of certainty that can be established at a given moment.

A variety of measures can be taken into consideration. Public statements following an attack, whether at the bilateral or local level (local démarches, cyber dialogues) or from Brussels (declarations of the spokesperson or of the High Representative, European Council conclusions or other statements) can be made without assigning responsibility. The country from whose territory the attack originates should be informed about the attack and required to provide information or take measures to stop the malicious activity. The EU has already made progress in developing common diplomatic messages that could be used by spokespersons or embassies in case of cyberattacks, but more needs to be done over the next months to advance further in this respect. When publicly assigning responsibility, the level of proof would necessarily need to be very high.

Work towards common threat assessments and a common culture of attribution

Achieving an EU collective response to a cyberattack does not require that all member states have their own independent in-depth analysis of the technical data. As in other cases, member states can decide to support a common decision based on the evidence and analyses provided by one or a group of member states.

While the public attribution of malicious cyber activities will ultimately remain a political decision, one which will continue to be influenced by a number of considerations, member states and EU institutions should do more to reach a common threat assessment and develop a shared culture of attribution. For this, **the sharing of information both between the EU member states and with the EU institutions is fundamental**. This mostly concerns intelligence sharing between the member states, but a strengthening of the analytical capabilities at the level of the EU INTCEN[37] is also necessary. INTCEN, working closely with the member states and EU institutions, is responsible for gathering and analysing all-source information available and preparing a political assessment about the events, which is meant to

provide the shared situational awareness needed for the decision-makers. In order to improve the decision-making mechanism, the use of the toolbox should also be exercised in table top exercises, involving the member states and the European institutions with responsibilities in this area.

Member states and EU institutions should do more to reach a common threat assessment and develop a shared culture of attribution.

While the implementing guidelines of the Cyber Diplomacy Toolbox do not attempt to harmonise the different methods, procedures, definitions and criteria used by the member states, "as attribution is a sovereign process", it is necessary to continue the work on common definitions and taxonomy for cybersecurity incidents. Using different methods and procedures to analyse cyberattacks can have benefits, but taking consequential political decisions based on different definitions and criteria could prove challenging.

More attention should also be given to establishing clearer criteria about what type of incidents need to be reported to authorities and to developing incentives for businesses and other private actors to (fully) report incidents and losses. The reporting systems need to be improved and provide the necessary degree of confidentiality.

Calibrating the objectives of sanctions

While not reacting to cyberattacks would encourage similar behaviour, **cyber sanctions will have to be used carefully and their goals should be clear from the start**. The proportionality of the EU response is one of the principles of the toolbox. While a change in behaviour would not be the only purpose of sanctions, in many cases it would be the main objective. If sanctions are used and they do not have the necessary effect of changing the behaviour of the target government, entity or individual, the credibility of the sanctions regime may be affected. However, the EU might still choose to adopt and maintain the sanctions, as they would also have the role to signal to the target, to EU citizens and to the international community what the EU considers (un)acceptable behaviour in this field.

The possible reaction from the sanctioned party will undoubtedly also play a role in the political assessments prepared before a decision is taken. The attribution of attacks and the use of sanctions can potentially worsen relations and affect cooperation on cyber issues with the particular country concerned. For instance, in 2014, after the US government accused China of hacking American major industrial companies such as U.S. Steel and Westinghouse Electric and brought criminal charges against Chinese military officials, China cancelled US-China cybersecurity dialogue activities[38], until the two countries reached a new cyber agreement in September 2015.

At the same time, not reacting to cyberattacks is likely to encourage similar or even more damaging behaviour. In this sense, attribution has a signalling role and even the existence of the Cyber Diplomacy Toolbox, with its sanctioning tool, points to the possible consequences of attacking EU entities. As such, it is intended to play a role in the calculations of potential aggressors, acting as a deterrent against bad behaviour.

While cyber sanctions could be adopted without publicly attributing an attack to a specific country, if attribution is made, it would be damaging for the EU's credibility if no measures would be taken. At the same time, given the difficulty of achieving unanimity among the EU member states in complicated cases, for the time being it may be more realistic to expect group attributions, in which a number of EU member states, but not all, would attribute an attack. While this would be better than no attribution, it would also signal that the EU is not managing to respond as a united actor.

Not reacting to cyberattacks is likely to encourage similar or even more damaging behaviour.

Any cyber sanctions listings will need to have clear objectives and EU member states will also need to agree on an exit strategy. The October 2018 non-paper mentions that sanctions could be lifted in response to a change in behaviour, the closing of an organisation at the origin of cyberattacks, a government taking stronger actions against perpetrators or making a political pledge to cease malicious activities. Reality will undoubtedly prove even more complicated and messier than these cases suggest.

Cyber sanctions listings will need to have clear objectives and EU member states will also need to agree on an exit strategy.

It is imperative that the future sanctions listings would be based on strong compelling evidence, which would withstand a case before the European Court of Justice (ECJ). Given the public nature of cases at the ECJ, the intelligence supporting a listing would need to be in the public domain, and thus cooperation with cybersecurity companies will be key for future work on this issue.

Working with the private sector

More generally, EU member states should continue to invest in a close dialogue with the private sector. Most cyber activities take place over infrastructures owned and operated by private companies. The private sector is among

the most impacted by state-sponsored malicious cyber activities and private companies are often better placed to provide deep technical analyses of these activities.

The Commission's proposal for the establishment of a Cybersecurity Competence Community to involve research entities, industry and the public sector has the potential to improve private-public cooperation. The Community is expected to give input to a Competence Centre that, among other things, will provide financial support and technical assistance to cybersecurity start-ups and SMEs.

Working with international partners

At the same time, the EU needs to continue to invest resources in global, regional and bilateral cyber dialogues, in the creation of common norms at the UN level and to try to broaden its use of confidence-building measures in this field. Reaching consensus at the UN level will not be easy given that discussions on the topic have been split up into two working groups set up as a result of competing resolutions, sponsored respectively by Russia and the US. This means developing relations with like-minded countries and investing in regional dialogues will be even more important.

NATO-EU cooperation is also crucial in this respect. Cooperation should move beyond the organisation of parallel exercises to organising truly joint ones. The two organisations need to also improve their coordination in terms of detection, attribution and response. While NATO does not have the same political or economic tools to deal with cyberattacks below the threshold of an armed attack as the EU has, the two organisations have much to learn from each other and should coordinate their responses and messages in reaction to significant cyberattacks. Given the UK's extensive capabilities, experience and activism in this field, Brexit will leave a significant gap in the EU's cyber capabilities and will impact the Union's ability to take common measures in this area. It will thus be vital for the two parties to continue to cooperate on cybersecurity after Britain's exit from the EU.

Brexit will leave a significant gap in the EU's cyber capabilities and will impact the Union's ability to take common measures in this area.

6. Conclusions: The need for common EU action

Though there are different views and levels of ambition among the member states on the issue of the cyber diplomacy toolbox, substantial progress has been made over the last couple of years. EU member states have adopted a cyber diplomacy toolbox containing a number of measures, from preventive ones to the possible use of sanctions. They now have the responsibility to finalise the cyber diplomacy framework that would allow them to take collective measures against threats that will undoubtedly only grow in magnitude and complexity.

Member states and EU institutions should do more to develop common threat assessments and a common culture of attribution of cyberattacks.

One of the key enablers for collective diplomatic action at EU level will be the necessary strengthening of cyber capabilities, both defensive and offensive. This will involve investment in human and technical capabilities, but also in creating and updating internal procedures so that the work of cybersecurity professionals feeds into the political decision-making process.

The attributions of cyberattacks will remain political decisions for national leaders to take and, like most foreign policy decisions, they will be influenced by diverse (geo)political considerations. However, to overcome hurdles of collective action and achieving unanimity in the EU Council for a common EU diplomatic response to cyberattacks, the member states and EU institutions should do more to develop common threat assessments and a common culture of attribution of cyberattacks. For this, the member states will need to upgrade their information sharing but also to use the Cyber Diplomacy Toolbox in table top exercises that simulate real-world scenarios.

While achieving agreement between the EU 27/28 on attributing cyberattacks to non-EU countries will continue to be challenging in the short term, the EU member states will still be able to use most of the framework's tools. These include preventive and cooperative measures even before a cyberattack takes place. During and after a cyberattack, the EU might employ measures such as statements and diplomatic démarches, with possible restrictive measures (sanctions) following later. These measures will have to be used carefully and based on strong compelling evidence.

While attributing attacks or adopting sanctions can potentially worsen relations with the particular country concerned, not reacting to cyberattacks is likely to encourage similar or even more damaging behaviour.

The EU Cyber Diplomacy Toolbox, with its attribution and sanctioning tools, has a signalling role and will likely feature in the calculations of potential aggressors, acting as a deterrent.

The EU will need to set up an enhanced cybersecurity cooperation with post-Brexit Britain and further develop EU-NATO cooperation in this field. At the same time, continued investment in confidence-building measures, in the development of norms at the UN level and in global, regional and bilateral cyber dialogues will be crucial to limit some of the more alarming developments occurring in cyberspace.

While the Cyber Diplomacy Toolbox is complementary to actions at the national level, acting together would allow the member states to send a stronger deterrent message. By responding as a united actor to common cyber threats, EU member states will be able to defend their security, their political and economic interests and further enhance the Union's credibility as an international actor.

[1] Andy Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar", *Wired*, 20 June 2017.

[2] "Cyber-attack: US and UK blame North Korea for WannaCry", *Reuters*, 25 May 2017; "Newly discovered vulnerability raises fears of another WannaCry", *Reuters*, 25 May 2017.

[3] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, 22 August 2017.

[4] "Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland and Renault in France", *The Independent*, 13 May 2017; Rosemain, Mathieu, Le Guernigou, Yann and Davey, "Renault stops production at several plants after ransomware cyber attack as Nissan also hacked", *Mirror Online*, 13 May 2017; "Honda halts Japan car plant after WannaCry virus hits computer network", *Reuters*, 21 June 2017.

[5] "Cyber-attack: Europol says it was unprecedented in scale", *BBC News*, 15 May 2017.

[6] Danny Palmer, "Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk", *ZDNet*, 16 August 2017.

[7] Paul Roberts, "NotPetya Infection Left Merck Short of Key HPV Vaccine", *The Security Ledger*, 27 October 2017.

[8] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, 22 August 2017.

[9] Council of the European Union conclusions (2018), "EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises", 10086/18, 26 June 2018.

[10] Cyber attribution is the process of tracking, identifying and laying blame on the perpetrator of a cyberattack.

[11] Council of the European Union (2016), "Non-paper: Developing a joint EU diplomatic response against coercive cyber operations", 5797/6/16, REV 6, 19 May 2016.

[12] Council of the European Union (2017), "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")", 10474/17, 19 June 2017.

[13] Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities. The 9 October 2017 draft version is the latest version of the document available online.

[14] The UN GGE – the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security is the UN-mandated working group in the field of information security.

[15] United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015.

[16] United Kingdom Foreign & Commonwealth Office, National Cyber Security Centre, and Lord Ahmad of Wimbledon, Foreign Office Minister condemns Russia for NotPetya attacks, 15 February 2018; Bussoletti, Francesco, "All Five Eyes countries have blamed Russia for the NotPetya cyber attack", *Difesa&Sicurezza*, 16 February 2018; Stilgherrian, "Blaming Russia for NotPetya was coordinated diplomatic action", ZDNet, 22 April 2018.

[17] Government of Canada, Communications Security Establishment, CSE Statement on the NotPetya Malware, 15 February 2018.

[18] European Council conclusions, 18 October 2018.

[19] Joint statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian cyber attacks, 4 October 2018.

[20] Various interviews with EU member states officials, October 2018-January 2019.

[21] Interviews with EU member states officials, January 2019.

[22] Knapton, Sarah, "Home Office blames North Korea for devastating NHS 'WannaCry' cyber attack", *The Telegraph*, 27 October 2017 and Bossert, Thomas P., "It's Official: North Korea Is Behind WannaCry", *The Wall Street Journal*, 18 December 2017.

[23] Foreign & Commonwealth Office, National Cyber Security Centre, and The Rt Hon Jeremy Hunt MP, Press Release, UK and allies reveal global scale of Chinese cyber campaign, 20 December 2018.

[24] Cimpanu, Catalin, "How US authorities tracked down the North Korean hacker behind WannaCry", *ZDNet*, 6 September 2018; The United States Department of Justice, Office of Public Affairs, North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, 6 September 2018.

[25] Interview with EU member state official, January 2019. Foreign & Commonwealth Office, National Cyber Security Centre, and The Rt Hon Jeremy Hunt MP, Press Release, "UK and allies reveal global scale of Chinese cyber campaign", 20 December 2018.

[26] Interview with EU member states officials, October 2018-January 2019.

[27] Guarascio, Francesco, "Italy resisting EU push to impose sanctions over cyberattacks", *Reuters*, 12 October 2018 and interviews with EU member states officials, October 2018-January 2019.

[28] Sanctions decisions and regulations usually contain annexes that list the individuals or organisations sanctioned. The action of adding entities to the sanctions list is referred to as 'listing'. Their elimination from the list, 'de-listing'. The sanctions regimes contain the reasons and the criteria on the basis of which entities are listed.

[29] EU Cyber Restrictive Measures: DK/EE/FI/LT/LV/NL/RO/UK non-paper, October 2018.

[30] EU Council, Council Decision (CFSP) 2018/1544 of 15 October 2018 concerning restrictive measures against the proliferation and use of chemical weapons. In December 2018, the EU foreign ministers have also given their political consent to a Dutch proposal to introduce a new sanctions regime targeting human rights abuses worldwide.

[31] Interviews with EU member state cyber diplomats, January 2019. Cerulus, Laurens, "Europe hopes to fend off election hackers with 'cyber sanctions'", *Politico Europe*, 11 February 2019.

[32] Computer forensics is a subdivision of digital forensic science, which aims to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions about the digital information found.

[33] Interview with EU member state cyber diplomat, January 2019.

[34] United States Department of Defense, "Cyber Strategy. Summary", 2018.

[35] Pearce, Rohan, "Cyber minister pushes 'forward defence' for Australia", *Computerworld*, 7 August 2018.

[36] The definition of the new concept of defending forward is still being debated. Defending forward would involve the conduct of cyber operations outside one's country networks and with lower limitations on the use of offensive tools, the aim being to stop cyber threats before they reach their targets.

[37] The EU Intelligence Analysis Centre (EU INTCEN) is the civilian intelligence body of the European Union, located in the European External Action Service.

[38] Daly, Robert, Weihua, Chen, Creemers, Rogier, "Is Indicting Chinese Hackers a Smart Move or Dumb Strategy?", *Foreign Policy*, 20 May 2014.

NOTES

NOTES

MISSION STATEMENT

The **European Policy Centre** is an independent, not-for-profit think tank dedicated to fostering European integration through analysis and debate, supporting and challenging European decison-makers at all levels to make informed decisions based on sound evidence and analysis, and providing a platform for engaging partners, stakeholders and citizens in EU policymaking and in the debate about the future of Europe.

The **Europe in the World Programme** scrutinises the impacts of a changing international system on Europe and probes how the EU and its member states can leverage their untapped potential to advance their interests and values on a regional and global level. It thus examines the evolution of EU relations with major powers, such as the United States, China and Russia, and how Europe can contribute to a rules-based global order. Second, the Programme focuses on the role of the EU in fostering reforms, resilience and stability in neighbouring regions. It looks closely at the developments in Turkey and Ukraine. Third, the Programme examines how the EU can strengthen its security in the face of terrorism, jihadist radicalisation or hybrid and cyber threats. It also seeks to advance the debate on Europe's defence policy.

With the strategic support of King Baudouin Foundation
Working together for a better society

With the support of Europe for Citizens Programme of the European Union