SWP Comment
NO. 19 APRIL 2018

The EU as a Force for Peace in International Cyber Diplomacy

Annegret Bendiek

Ever since the cyber attacks against the computer networks of European governments and defence and foreign ministries have become public knowledge, security policy-makers have insisted that the EU Member States need to develop more adequate cyber-defence and cyber-retaliation capabilities. However, the EU continues to base its cyber-security strategy on the resilience of Information and Communication Technology Infrastructures and cyber diplomacy as part of its Common Foreign and Security Policy (CFSP) so as to position itself as a force for peace. Its Joint EU Diplomatic Response to Malicious Cyber Activities, adopted in October 2017, primarily stipulates non-military instruments that could contribute to "the mitigation of cybersecurity threats, conflict prevention and greater stability in international relations". Faced with increasing activities infrastructures, Europe would be well-advised to adhere to the step-by-step cyber-diplomacy plan, which is based on the principle of due diligence.

Cyber attacks, such as against the information and telecommunications infrastructure of the German federal government, cyber-espionage, intellectual property theft, cybercrime or disinformation not only paralyse single communication and cybersecurity policies, they can also constitute part of hybrid warfare. "Hybrid" here means the deliberate covert or overt use of civilian and military instruments by state or non-state actors. Alongside cyber attacks, these include disinformation campaigns, espionage, economic pressure, the use of proxy forces and other subversive activities. Therefore, after the nerve-gas attack in London, EU heads of government and state declared their unequivocal solidarity with the United Kingdom in late March 2018 and threatened Russia with consequences. Further sanctions are being considered, as is digital retaliation (hackback).

Cyber Defence: Defensive or Offensive?

It is a politically and legally controversial issue whether attacked states should adopt offensive countermeasures, such as hack-backs, to neutralise the source of a cyber-attack. Germany's 2016 Cyber Security Strategy pledged the need for defensive

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

cyber security and calls for the creation of a mobile Quick Reaction Force housed within the Federal Office for Information Security (BSI), as well as similar teams within the federal police and domestic intelligence agency that are able to respond to cyber threats against government institutions and critical infrastructure. The new coalition government takes the stance that the state requires military and strategic cyber weapons as well as a legal basis for their deployment in order to respond to cyber attacks, such as on the federal parliament in 2015 or the government network in 2016.

NATO categorises attacks in cyberspace as a form of warfare, which can trigger the mutual defence clause under Article 5 of the North Atlantic Treaty. NATO is currently debating whether offensive computer-network operations by its member states should be a component of its operational planning. Since the 2016 NATO Summit in Warsaw, NATO-EU cooperation has been strengthened through the exchange of information and joint cyber-security exercises. In its 2016 Paper on German Security Policy and the Future of the Bundeswehr, the German federal defence ministry extended this development and created a sixth organisational unit for its military — the cyberspace and information space unit — which currently has approximately 13,500 staff. In the case of self-defence or mutual defence within NATO, both defensive and offensive cyber-defence capabilities may be used. Whether this holds true for offensive capabilities in peacetime is contentious. Critics argue that the proliferation of malware for cyber-attacks does not justify the short-term advantages generated by the supposedly greater potential for deterrence which these capabilities offer. They insist that confidence and security-building measures as well as arms control must be led by the United Nations (UN) and OSCE, and that any development of offensive cyber-defence capabilities risks fuelling mistrust, mutual insecurity and conflicts. They believe that only a long-term cyber diplomacy coordinated at the European level could help to bring about security in Europe and avoid conflict escalation. Self-evidently, it is in the EU's own interests to position itself as a force for peace in cyber security and to emphasise compromise and communication.

Cyber-Diplomacy Formats

Cyber diplomacy — as opposed to overall cyber defence — offers the potential for conflict de-escalation and thus for developing a force for peace. More than 30 states now have commissioners for cyber foreign policy. Denmark has even appointed a cyber-diplomacy ambassador. Cyber diplomacy in the widest sense encompasses confidence-building measures (CBMs). It also comprises certain aspects of international norm building, data protection and freedom of expression, Internet Governance, and prosecution under international agreements for mutual legal assistance. Many governments, however, have neither the knowledge nor the necessary resources to maintain basic cyber-security standards or even ascertain what attacks are being conducted via servers on their territory. Nevertheless, most states voice profound reservations over national sovereignty when presented with the idea of a central global regulatory body for security in cyberspace, thereby rendering it an unrealistic prospect for the time being. It is more likely that cyberspace and information space will be increasingly subject to national sovereignty.

On the multilateral level, in 2015 a group of 25 international government experts commissioned by the UN General Assembly reached a consensus that international law should be applied in cyberspace as well, including the right to self-defence. However, in summer 2017 the group could not agree on whether to establish a so-called attribution council. As a precondition for attribution — meaning the technical, legal and political identification of the perpetrator of a cyber attack — sensitive information must be exchanged among Computer Emergency Response Teams (CERTs) and between secret services and security agencies.

Due to ineffective multilateral formats, in 2016 presidents Xi Jinping and Vladimir Putin signed a bilateral joint declaration in Shanghai announcing a new phase in the comprehensive strategic partnership between China and Russia. Beijing and Moscow voiced their concern that information and telecommunications technologies were being misused for interference in internal affairs. The international community, they stated, should cooperate on the basis of mutual respect and expediency as well as justice, and provide joint responses to threats to information security. The US also relies on bilateral agreements, for instance with China, to fight cybercrime.

Ever since multilateral negotiations at the UN level failed in 2017, cyber-security experts have been calling for "coalitions of the willing" from G20 or G7 states to drive international norm-setting forward. Two-track formats, such as the Global Commission on the Stability of Cyberspace, predominate. However, strengthening attribution concerns not only states but also the private sector. In February 2017 Microsoft called for a "Digital Geneva Convention". The most recent initiative, a "Charter of Trust" launched by Siemens at the Munich Security Conference in February 2018, sets the same course. Finally, the World Economic Forum aims to create a Global Centre for Cybersecurity to combat cybercrime and thus also improve cooperation between the private sector and state authorities, the so-called public-private partnerships.

The EU's Cyber-Foreign and Cyber-Security Policy

Cyber security is an issue not only for states but for the EU as well. It extends beyond the resilience of networks, the digital single market or the prosecution of cyber criminals, and also concerns the EU's Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP) (see table on next page). A range of actors already tackle cyber-foreign and cyber-security policy within the EU's Integrated Political Crises Response (IPCR): most significantly, the EU Agency for Network and Information Security (ENISA); the European Cybercrime Centre (EC3) at Europol; the EU Intelligence and Situation Centre (INTCEN); the Intelligence Directorate of the EU Military Staff (EUMS INT) and its situation room (SITROOM); the INTCEN unit for analysing hybrid threats, known as the Hybrid Fusion Cell; the Computer Emergency Response Team for EU institutions and agencies (CERT-EU); and the European Commission's Emergency Response Coordination Centre (ERCC). New structures and mechanisms created under the Network and Information Security (NIS) directive, such as the member states' network of IT emergency teams (CSIRTs), must also be acknowledged.

At the EU level, the Horizontal Working Party on Cyber Issues was created in 2015 to coordinate the political aspects of cyberspace within the Council. It can participate in both legislative and non-legislative activities. Furthermore, EU member states decided in February 2015 to strengthen cyber diplomacy at the EU level in the European External Action Service (EEAS). This was confirmed in November 2016 by the implementation plan on security and defence. Important bodies that coordinate the strategic upstream analysis for the CFSP are the cyber diplomacy team in the EEAS as well as EU INTCEN for civilian situational awareness and EUMS INT for the military. To deter and reconstruct cyber attacks, and identify the perpetrators, forensic computer scientists depend on numerous sources in different states and companies on all political levels. To establish coordination in this area, the EU can rely on well-established cooperation between ministries and security agencies. Special rules apply for the fight against terrorism. However, an EU-coordinated policy that brings together binding exchanges of information with surveillance and the use of that shared information has not yet been enshrined as an EU competence in the treaties but is subject for reconsideration. The EU's Joint Communication on "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the

Table

Cyber Security in the EU: Areas of Responsibility

	Peace, security, justice	*Single market*	*CSDP: Cyber Defence*	*CFSP: Cyber Diplomacy*
EU	Europol (EC3) Eurojust EU-LISA	ENISA CSIRT network CERT-EU	EDA GSA	EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU Hybrid Fusion Cell ERCC
National	Executive and data-protection authorities	Authorities in charge of NIS National CSIRTs	Defence, military and security agencies	Foreign ministries

CERT: Computer Emergency Response Team, *CSIRT*: Computer Security Incident Response Team, *EC3*: European Cybercrime Centre, *EDA*: European Defence Agency, *EEAS*: European External Action Service, *ENISA*: European Union Agency for Network and Information Security, *ERCC*: Emergency Response Coordination Centre, *EU INTCEN*: European Union Intelligence and Situation Centre, *EU-LISA*: European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice, *EU SITROOM*: European Union Situation Room, *EUMS INT*: European Union Military Staff, Intelligence Directorate Mission, *GSA*: European Global Navigation Satellite Systems Agency, *NIS*: Network and Information Security, *SIAC*: Single Intelligence Analysis Capacity.

EU” of September 2017 offers starting-points for cooperation that builds both confidence and security and is based on the four pillars of EU cyber security (see table). The Horizontal Working Party on Cyber Issues, chaired by the rotating Presidency, and the Political and Security Committee (PSC) are responsible for appropriate implementation measures. Legally Member States are free to launch initiatives.

First pillar: The provisions of the Directive on Attacks against Information Systems of 2013 including its penalties are applicable in the case of criminal actors without significant ties to a State sponsor. To counter the growing threat of cross-border cybercrime, new instruments are planned that can be used to prosecute perpetrators more effectively. An “e-evidence” directive is currently being negotiated to facilitate cross-border access to electronic evidence. Also under discussion is a directive on fighting fraud and forgery in cashless media, such as bitcoin. This aims to improve cooperation between criminal-justice authorities.

Second pillar: ENISA is being upgraded, having increased its staff from around 80 to 125 and its annual budget from 11 to 23 million euros. The agency is expected to organise yearly pan-European cyber-security exercises and steer cooperation between the member states’ Computer Security Incident Response Teams (CSIRTs). Previously, these exercises were occasionally extended to allied non-member states. ENISA is primarily meant to accompany the establishment and implementation of an EU-wide certification framework. The objective is to make IT products and services more secure through market incentives and to enable users to make informed purchasing decisions. Divergent certification systems will be harmonised to strengthen the digital single market for trustworthy products. These measures are based on the Network and Information Security (NIS) directive, which will come into force in May 2018; it serves as a benchmark for attaining similar improvements in the OSCE as well.

Third pillar: In December 2017 the EU’s 25 defence ministers established Permanent Structured Cooperation (PESCO). Two of its 17 projects are explicitly dedicated to Europe’s cyber security. According to reports, others concern the standardisation of soldier systems — meaning electronic equipment, linguistic and data communications, and software. Greece plans to develop a European IT emergency team; Lithuania wants to be in charge of establishing a European cyber defence. The idea is to create a "cyber Schengen area" so as to combat online criminality operating across all national borders. By late 2020 the European Investment Bank intends to invest more than 6 billion euros in developing so-called dual-use technologies for cyber security and civilian security.

Fourth pillar: The EU is conducting bilateral cyber dialogues within its strategic partnership agreements with USA, Canada, China, South Korea etc. The EU also proposes drawing up a strategy for international cooperation in cyberspace and conflict prevention, in line with the cybersecurity reform of September 2017. As a first step, it has updated the CFSP and CDSP's instruments as well as its directive on export controls for dual-use goods.

Joint EU Diplomatic Response to Malicious Cyber Activities

The increase in cyber attacks has forced international actors to consider how to respond appropriately. The Obama administration imposed unilateral sanctions for the first time in 2014 after a US subsidiary of the Sony Corporation fell victim to a devastating cyber attack, during which all company data were copied. Two years later, Washington reacted similarly when the US administration's personnel data were siphoned during a large-scale cyber attack. Following the alleged Russian interference in the 2016 US presidential election campaign, the US government imposed sanctions in March 2018 on five companies and organisations as well as 19 individuals, citing Russia's "malicious cyber activities". The EU had first discussed the necessity for joint cyber diplomacy in February 2015. In June 2017, it suggested establishing a Cyber Diplomacy Toolbox so as give the EU a joint diplomatic response to malicious cyber activities. Its main goal was to guarantee the responsiveness of its foreign and security policy below the threshold for armed conflict. This would complement its efforts under the NIS directive to push through minimum standards and reporting obligations as well as build resilient IT and communications systems in the digital single market. At the EU level, responding to attacks with cyber diplomacy above triggers the political measures contained in the CFSP, including restrictive measures. In October 2017, the planned Cyber Diplomacy Toolbox was adopted under its new title of Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities. Its purpose is to facilitate cooperation in containing immediate and long-term threats and to help deter culprits and potential attackers in the long term. Individual states apparently did not have sufficient reach to impact on attackers' cost-benefit calculations; EU diplomacy, by contrast, offered a strategic added value due to its ability to impose sanctions or positive incentives. The EU has committed to international principles upholding due diligence in cyberspace and intends to strengthen cyber diplomacy in exchanges with third parties with the aim of combating cyber attacks. The UN's Group of Governmental Experts (GGE) incorporated the principle of upholding due diligence in its final report of June 2015. According to this report, states should ascertain that their sovereign territory, and the computer systems and infrastructure located there or otherwise under their control, are not misused for attacks on the infrastructure of other states.

Five Categories of Measures

In its cyber diplomacy, the EU relies on the CFSP toolbox. Its measures can be divided into preventative, cooperative, stabilising and restrictive, as well as member states' lawful responses for self-defence. Political measures are agreed in the EU Council with the assistance of the European External Action Service. In grave instances, malicious cyber activities could amount to punitive measures and the use of force or an armed attack in accordance with international law and the Charter of the United Nations. In this case, member states take a sovereign decision to exercise individual or collective self-defence as recognised in Article 51 of the UN Charter and in accordance with international and humanitarian law.

Prevention: Within the EU's political dialogues with third states, it has developed cyber dialogues that aim to influence the behaviour and attitude of its dialogue partners. The EU also supports confidence-building measures (CBMs) such as those developed by the OSCE. Dialogues with regional organisations such as the African Union or ASEAN are particularly important. The EU and the respective regional body can define how to build up the region's capacities for using cyberspace (known as "cyber capacity building") in association, partnership or cooperation agreements, or even through the Instrument contributing to Stability and Peace (IcSP).

Cooperation: To facilitate an ongoing incident, an EU delegation in a host country can transmit a diplomatic note (démarche) to that country's government. This requires an instruction from the High Representative of the Union for Foreign Affairs and Security Policy. In a conflict situation, the delegation head can deliver a proposal to conduct comprehensive talks or merely convey key messages. Démarches can also be formulated and delivered together with third states. Where the EU delegation head has been recalled due to conflict, this type of cooperative solution is no longer possible.

Stability: These measures have a signalling function by serving as a strategic communication that the potential aggressor should refrain from engaging in malicious cyber activities The European Council can set out an EU act or position, but only unanimously. It can also pass a resolution to implement such an act. In that case, qualified-majority voting applies, except for acts of implementation concerning the military or defence (art 31 para 2 TEU). The High Representative of the Union for Foreign Affairs and Security Policy can also make a declaration "in the name of the EU". However, this has to be agreed beforehand with all EU states and is usually employed if there is no need for an immediate response, if the EU first has to work out its position vis-à-vis a new situation, or if it has modified an established position. However, the High Representative can also make a declaration under her own responsibility if a quick reaction is required but it is not possible to seek agreement from the EU 27.

Sanctions: The EU can impose restrictive measures (sanctions) if it intends to push through political objectives following serious cyber attacks. These measures tend to target government officials of third states, but also state companies or other legal or natural persons. Sanctions have to be voted unanimously in the Council and must conform to the CFSP's objectives under art 24 TEU. Sanctions can be divided itno two main categories: those decided autonomously by the EU and those that the EU is obliged to impose following a resolution by the United Nations Security Council. Under EU law, sanctions must be targeted. For instance, specific persons or companies may be put on a sanctions list in order to block their bank accounts as long as minimum rule-of-law standards are met. So-called prerequisites for legality have been drawn up for such cases, which stipulate, for example, that those targeted have to be informed of the reasons for being listed and be given the opportunity to file a complaint.

Possible EU support to Member States' lawful respsonses: The Lisbon Treaty introduced the solidarity and mutual-assistance clauses, which can be invoked after severe cyber attacks. The solidarity clause (art 222 TFEU) stipulates that EU member states provide mutual support if one or several of them are victims of terror attacks, natural disasters or man-made disasters (including serious cyber incidents). Its implementation procedure was defined by Council decision in July 2014. The mutual-assistance clause contained in art 42 para 7 TEU roughly corresponds to Article 5 of the NATO Treaty, although the latter takes precedence for NATO members. The mutual-assistance clause was invoked for the first time in November 2015 by France following the Paris terror attacks. Under the Joint EU Diplomatic Response to Malicious Cyber Activities of October 2017, responses that are compliant with international law do not require unequivocal attribution of cyber attacks to specific origins or perpetrators. This accords with the interpretations of international law experts enshrined in the Tallin 2 manual on how international law applies to cyberspace.

Export Controls

The EU intends to promote its cyber diplomacy and aspiration to due diligence by controlling the export of dual-use goods more strictly. The dual-use directive of May 2009 regulates the member states' joint licensing requirements for the export, procurement and transit of such goods. In mid-December 2017, the European Commission published a new version of the directive's annexes I, IIa to IIg and IV. The update mainly concerned new controls for certain goods, such as IT hardware. Goods are categorised as subject to control (annex I) based on a) the stipulations of international treaties and obligations, especially UN Security Council Resolution 1540, the Chemical Weapons Convention and the Biological Weapons Convention, and b) the control lists of international multilateral export regimes, above all the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australia Group and the Missile Technology Control Regime (MTCR). These lists in particular are constantly modified. Not only is the export of specific goods to states under sanction subject to tighter controls, but in many cases separate approval also has to be obtained for exporting dual-use goods. Non-compliance can result in stiff penalties or fines.

Due Diligence, Step by Step

The EU's unanimity requirement makes positioning it as a force for peace difficult. Its member states not only display great strategic ambivalence, for instance in their policy towards Russia, but their actions in foreign affairs also lack coherence. The EU's aspiration to act as a force for peace is shown by member states seeking to strengthen the due-diligence principle via the CFSP's political instruments. Due diligence is a well-accepted principle in international law based on the idea that the EU not only has to guarantee that rules are upheld in its own jurisdiction, but also needs to bear responsibility for the consequences of its actions beyond its borders, for instance through a stricter export policy. Ever more frequently, EU decisions reach beyond its jurisdiction. It is the EU's role — and its role alone — to create coherence in this area. Where protecting cyberspace is concerned, member states should not limit themselves to avoiding irresponsible solo decisions. They must also undertake everything that could reasonably be expected from them to contribute along with other states to an "open, global, free, peaceful and secure cyberspace".

There is debate over how far EU governments should prepare to take technical counter-measures or even carry out hackbacks, as is currently being considered in the case of Russia. This would be the highest level of escalation under the mutual-assistance clause when a Member State chooses to invoke self-defence as recognised in Article 51 of the UN Charter and in accordance with international law, including humanitarian law. The final step of crisis management would then consist of stopping an ongoing attack through active defence. *Ultima ratio* would be a so-called hackback, meaning the targeted elimination of the server from which an attack has been launched. This only complies with the principle of due diligence if the ongoing attack has serious consequences that threaten a state's survival and if all other means have been exhausted. The legal framework and the distribution of competences this requires have not been defined, not even at the national level.

The EU's most important and lastingly effective tools in this context are prevention and detection. Prevention encompasses the measures contained in the NIS directive, such as the introduction of minimum standards and reporting requirements for operators of critical infrastructure. Telecommunications providers are allowed to analyse data traffic in case of disturbances and, if necessary, block the culprits they identify.

Detection is the elucidation and attribution of attacks. Here, political evaluation is decisive. It has to take into account the overall picture of incidents in cyberspace to anticipate militarily relevant hybrid threats. Where professional attacks are concerned, cyber diplomacy between likeminded states is necessary for security agencies to be able to share analyses of code fragments and of the way the attack unfolded. Such analyses often make it possible to draw conclusions about hacker groups and their origins. The CSIRT network and its technical competence is meant to provide a similar exchange for Critical Infrastructure Protection. Cyber diplomacy also requires authorities and businesses to exchange information. Public and private CERT groups and alliances in industry are indispensable for pooling expert knowledge in cyber diplomacy as well.

Cyber diplomacy is an important component of national cyber security, but it also has to integrate the European and even global dimension. Investigations based exclusively on national information are insufficient. With its Joint EU Diplomatic Response Framework of 2017, the EU has opted for a non-military cyber-security policy. This helps resist the temptation to respond to threats in cyberspace immediately. Instead, the EU privileges political measures as part of the CFSP, so as to make its mark as a force for peace. This approach should be understood as a clear political signal by its partners and competitors worldwide.

Dr. Annegret Bendiek is a Senior Associate in the EU / Europe Division at SWP.

This Comment reflects the author's views.

The online version of this publication contains functioning links to other SWP texts and other relevant sources.

SWP Comments are subject to internal peer review, fact-checking and copy-editing. For further information on our quality control procedures, please visit the SWP website: https://www.swp-berlin.org/en/about-swp/quality-management-for-swp-publications/

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

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

ISSN 1861-1761

Translation by Tom Genrich

(English version of
SWP-Aktuell 22/2018)