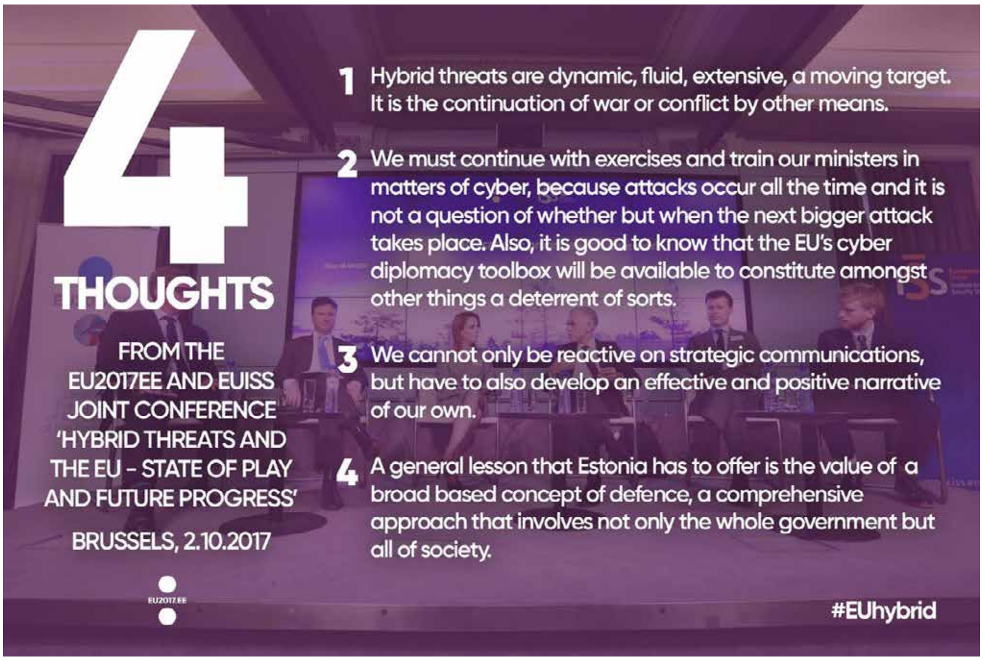
3.4 The EU as a partner in cyber diplomacy and defence

by Thomas Renard and Andre Barrinha

The European institutions became involved in cyber-related issues in the 1990s. However, cyberspace only came to be conceived as a security space a decade later. As late as 2003, cyber issues were not even mentioned in the European Security Strategy (ESS). That was to be progressively rectified with a number of non-binding communications from the European Commission, focusing mostly on the security of the EU's cyberspace.

More recently, the EU's cyber agenda has broadened considerably to embrace more systematically the international dimension of cyber issues. It adopted its first cybersecurity strategy in 2013, which included international priorities. It also adopted European Council conclusions specifically on 'cyber diplomacy' in 2015, marking the beginning of a more proactive role for the EU in international cyberspace policy-making. In 2017, the Council agreed to develop a full cyber-diplomacy 'toolbox', with the potential for approving retaliatory measures against cyber-attacks conducted or sponsored by other states.



4 THOUGHTS

FROM THE EU2017EE AND EUISS JOINT CONFERENCE 'HYBRID THREATS AND THE EU – STATE OF PLAY AND FUTURE PROGRESS'

BRUSSELS, 2.10.2017

1 Hybrid threats are dynamic, fluid, extensive, a moving target. It is the continuation of war or conflict by other means.

2 We must continue with exercises and train our ministers in matters of cyber, because attacks occur all the time and it is not a question of whether but when the next bigger attack takes place. Also, it is good to know that the EU's cyber diplomacy toolbox will be available to constitute amongst other things a deterrent of sorts.

3 We cannot only be reactive on strategic communications, but have to also develop an effective and positive narrative of our own.

4 A general lesson that Estonia has to offer is the value of a broad based concept of defence, a comprehensive approach that involves not only the whole government but all of society.

EU2017.EE

#EUhybrid

The development of the EU's global cyber agenda sits at the juncture of three key trends. First, the growing importance of cyber issues, which have progressively become core themes in Member States' agendas. Second, beyond domestic priorities, cyber issues have climbed the international agenda as well, becoming increasingly 'politicised'. Indeed, cyberspace has become an immensely contested area, confronting distinct national interests and visions for the digital age. Cyber issues were treated first as purely technical issues, then as external aspects of domestic policies, before being recognised as a major foreign policy topic. Third, the EU's own internal evolution, gradually developing itself as a diplomatic and security actor with global ambitions, is naturally leading to the development of global cyber ambitions and tools. This short contribution seeks to highlight key elements of that evolution.

The EU as a cybersecurity actor

The EU became interested in cybersecurity in the late 1990s, with a clear focus on cybercrime and its potential negative impact on the single market. Since the early 2000s, it has progressively expanded its interest and role in this domain, internally at first and subsequently externally. At the domestic level, the European Commission and the Council adopted a series of non-binding documents throughout the 2000s related to computer security, critical (information) infrastructure protection and even cyberterrorism. It was only at the turn of the first decade of the 21st century that cyberspace became a paramount political and strategic concern, leading the EU to agree on a number of key documents and legislation, such as:

- The 2005 Council Framework Decision on Attacks Against Information Systems;
- The 2010 EU Internal Security Strategy, which identified cybersecurity as one of its five strategic objectives;
- The 2013 EU Cybersecurity Strategy, which identified five strategic priorities: building resilience; fighting cybercrime; developing cyber defence policy; fostering industrial and technological resources; and embedding EU values in cyberspace;
- The 2015 Agenda on European Security, which defines cybercrime as one of its three priorities (together with serious organised crime and terrorism);
- The 2016 Network Information Security (NIS) Directive, which is the first EU-wide legislation on cybersecurity. It makes it mandatory for EU Member States:
  to be prepared and equipped to respond to cyber incidents (e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority); to cooperate swiftly and effectively among themselves in case of incidents, notably by sharing information; and to develop a 'cybersecurity culture' among critical sectors and businesses, with the obligation to notify security breaches.
- A reviewed EU Cybersecurity Strategy was adopted in September 2017, together with a package of new proposals. It focuses on the creation of new technological capabilities via research, innovation and skills development and on the improvement of cooperation at EU level.

At the external level, the EU's activity is more recent and to some extent more modest. The 2003 European Security Strategy, a key document that listed the main security challenges to the EU, did not even mention cyberspace. It was only the 2008 *Report on the Implementation of the European Security Strategy* that mentioned cyber as a potential challenge with an external dimension. High-scale cyber-attacks in the preceding months in both Estonia (2007) and Georgia (2008) certainly contributed to the progressive prioritisation of cyber issues on the security agenda. Four EU documents are particularly relevant and illustrative of the EU's growing focus on international aspects of cyber issues:

- The above-mentioned 2013 EU Cybersecurity Strategy called for a more active EU engagement on the international level, notably by deepening the dialogue with third countries and international organisations and by stepping up capacity-building programmes in third countries.
- The 2015 Council conclusions on cyber diplomacy promote a number of objectives and principles related to the EU's global cyber engagement: the promotion and protection of human rights in cyberspace; norms of behaviour and application of existing international law in the field of international security; internet governance; enhancing competitiveness and prosperity; capacity building and development; and strategic engagement with key partners and international organisations.
- The 2016 EU Global Strategy, the main guiding document for the EU's foreign policy, considers 'cyber' as one of the key constituents of Europe's security but also as a significant element in the EU's foreign policy (e.g. to build cyber resilience in the neighbourhood or to shape the global cyberspace).
- The 2017 Council conclusions on a 'cyber-diplomacy toolbox' affirm the EU's willingness to put to use the entire scope of CFSP measures, including restrictive ones (such as sanctions), in order to respond in a proportionate manner to cyber malicious activities by third parties, to protect the Union and to attain its foreign policy objectives.

In its pursuit of domestic and foreign cyber policies, the EU relies on a growing number of agencies that are particularly relevant. They include:

- The European Union Agency for Network and Information Security (ENISA), established in 2004, which strengthens EU Member States' cyber resilience through advice and capacity building;
- The EU Computer Emergency Response Team (CERT-EU), set up in 2012, which is in charge of the response to cyber incidents within EU institutions;
- Europol's European Cybercrime Centre (EC3), established in 2013 to strengthen the law enforcement response to cybercrime, notably through operational support;

- The European Defence Agency (EDA), which considers ‘cyber’ as one of its priorities and works on the cyber-defence capability development of its member states;
- The European Security and Defence College (ESDC), which has been in charge of education, training, evaluation and exercise in the field of cybersecurity and defence (cyber ETEE platform) since 2018 and is therefore tasked with providing cyber-related training to civilian, police and military staff, in line with CSDP requirements.

Cyber diplomacy and cyber partnerships

Cooperation in cyberspace is a choice, not a given. In 2011, Barack Obama wrote in the introduction to the US *International Strategy for Cyberspace* that *‘by itself, the internet will not usher in a new era of international cooperation. That work is up to us.’* Indeed, cyberspace is a disputed domain. More than 30 countries worldwide are said to have developed offensive cyber capabilities, and that number is growing. Countries are also promoting very distinct models for internet governance. On the one hand, some countries, including most EU Member States, are promoting a vision of a free and open internet, whereas on the other hand, countries such as Russia and China seek to assert more government control over the internet.

In this context, and with a view ‘to promot[ing] openness and freedom of the internet’ and *‘to encourag[ing] efforts to develop norms of behaviour and apply existing international laws in cyberspace’*, as stated in the 2013 Cybersecurity Strategy, the EU has deepened its engagement with a number of strategic partners.

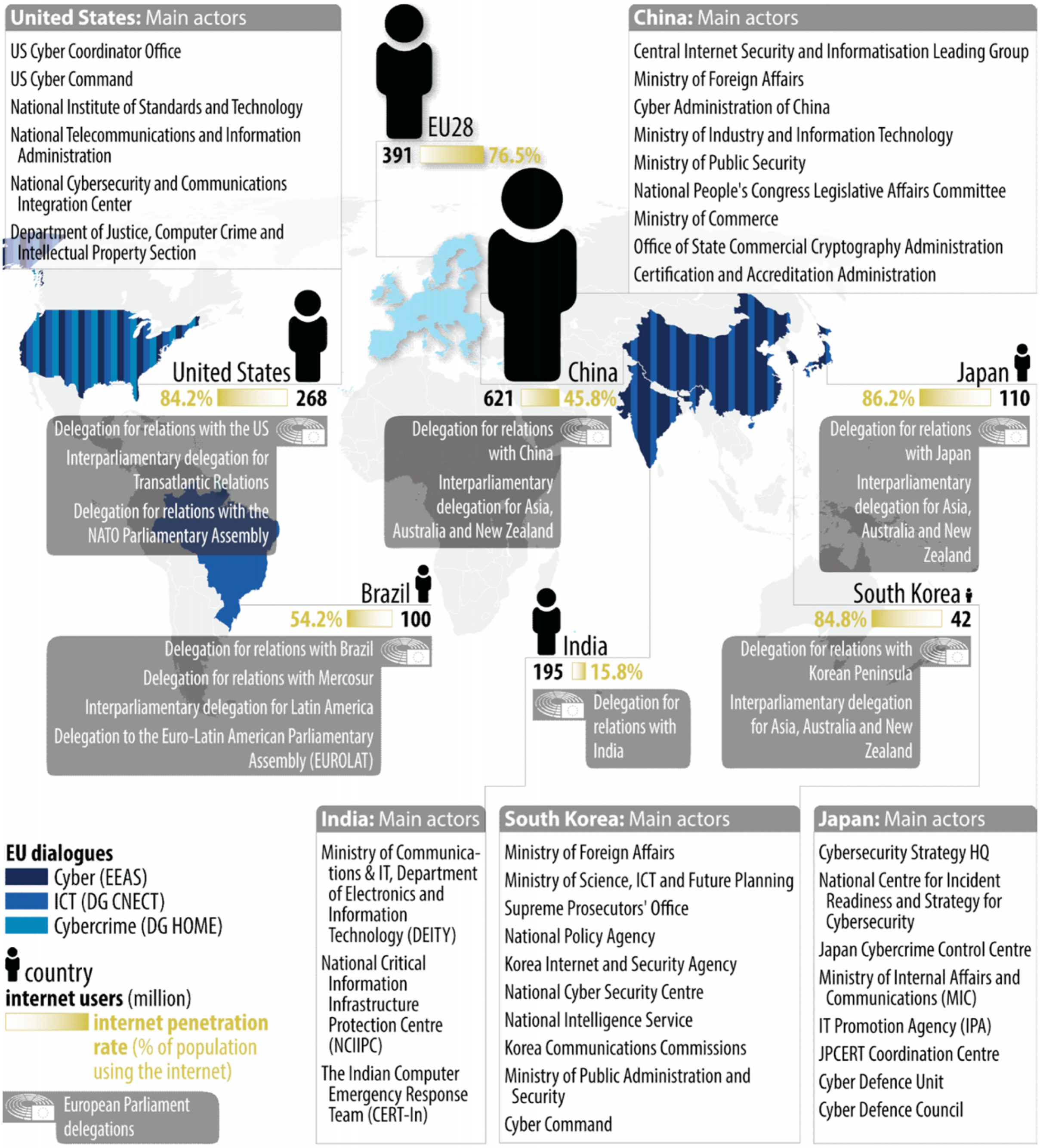
Photo: European Union, 2018 / EC - Audiovisual Service / Lukasz Kobus

The EU has deepened its engagement in cyberspace with a number of strategic partners.

It has formalised a number of partnerships with third countries by establishing regular policy dialogues on cyber issues and by adding a cyber chapter to the joint cooperation agenda, when there is one (such as the EU-China 2020 Strategic Agenda for Cooperation). Not all partnerships deliver equally, however. The EU-US cyber partnership is by far the oldest and most developed, with several annual dialogues covering various aspects of cyber policies. It is also the only partnership singled out in the EU Cybersecurity Strategy as well as in the EU Global Strategy. The partnerships with Japan and to a lesser extent Canada are less ambitious but still productive in a 'like-minded' context, as also illustrated by the 2017 G7 Lucca declaration on responsible state behaviour in cyberspace. Conversely, cyber partnerships with China and Russia are less straightforward. These two countries are perceived as major sources of cyber-attacks and cyber-espionage in Europe. As mutual trust is lacking, cooperation focuses mostly on confidence-building measures. This is one of the key aims of the EU-China cyber taskforce, as well as of the track 1.5 Sino-European Cyber Dialogue (SECD). Cooperation with other 'strategic partners', such as India or Brazil, remains largely under-delivering.

Such an observation would fundamentally challenge the notion of cyber partnership, were it not for the distinction between results-oriented and process-oriented partnerships. Whereas the transatlantic partnership aims for tangible deliverables, such as increasing cybersecurity in the transatlantic space and beyond, the partnerships with China and Russia mostly seek to keep the dialogue open on contentious issues, and possibly aim to build mutual confidence. Having said this, most cyber partnerships ultimately operate a balance between results and process. Even the EU-US partnership seeks to strike this balance, as it is still hampered by a serious trust deficit.

Map 1 – EU's cyber-related dialogues with third countries



United States: Main actors

- US Cyber Coordinator Office
- US Cyber Command
- National Institute of Standards and Technology
- National Telecommunications and Information Administration
- National Cybersecurity and Communications Integration Center
- Department of Justice, Computer Crime and Intellectual Property Section

China: Main actors

- Central Internet Security and Informatisation Leading Group
- Ministry of Foreign Affairs
- Cyber Administration of China
- Ministry of Industry and Information Technology
- Ministry of Public Security
- National People's Congress Legislative Affairs Committee
- Ministry of Commerce
- Office of State Commercial Cryptography Administration
- Certification and Accreditation Administration

United States:

- Delegation for relations with the US
- Interparliamentary delegation for Transatlantic Relations
- Delegation for relations with the NATO Parliamentary Assembly

China:

- Delegation for relations with China
- Interparliamentary delegation for Asia, Australia and New Zealand

Japan:

- Delegation for relations with Japan
- Interparliamentary delegation for Asia, Australia and New Zealand

Brazil:

- Delegation for relations with Brazil
- Delegation for relations with Mercosur
- Interparliamentary delegation for Latin America
- Delegation to the Euro-Latin American Parliamentary Assembly (EUROLAT)

India:

- Delegation for relations with India

South Korea:

- Delegation for relations with Korean Peninsula
- Interparliamentary delegation for Asia, Australia and New Zealand

EU dialogues

- 🟦 Cyber (EEAS)
- 🟦 ICT (DG CNECT)
- 🟦 Cybercrime (DG HOME)

country
internet users (million)
internet penetration rate (% of population using the internet)
European Parliament delegations

India: Main actors

- Ministry of Communications & IT, Department of Electronics and Information Technology (DEITY)
- National Critical Information Infrastructure Protection Centre (NCIIPC)
- The Indian Computer Emergency Response Team (CERT-In)

South Korea: Main actors

- Ministry of Foreign Affairs
- Ministry of Science, ICT and Future Planning
- Supreme Prosecutors' Office
- National Policy Agency
- Korea Internet and Security Agency
- National Cyber Security Centre
- National Intelligence Service
- Korea Communications Commissions
- Ministry of Public Administration and Security
- Cyber Command

Japan: Main actors

- Cybersecurity Strategy HQ
- National Centre for Incident Readiness and Strategy for Cybersecurity
- Japan Cybercrime Control Centre
- Ministry of Internal Affairs and Communications (MIC)
- IT Promotion Agency (IPA)
- JPCERT Coordination Centre
- Cyber Defence Unit
- Cyber Defence Council

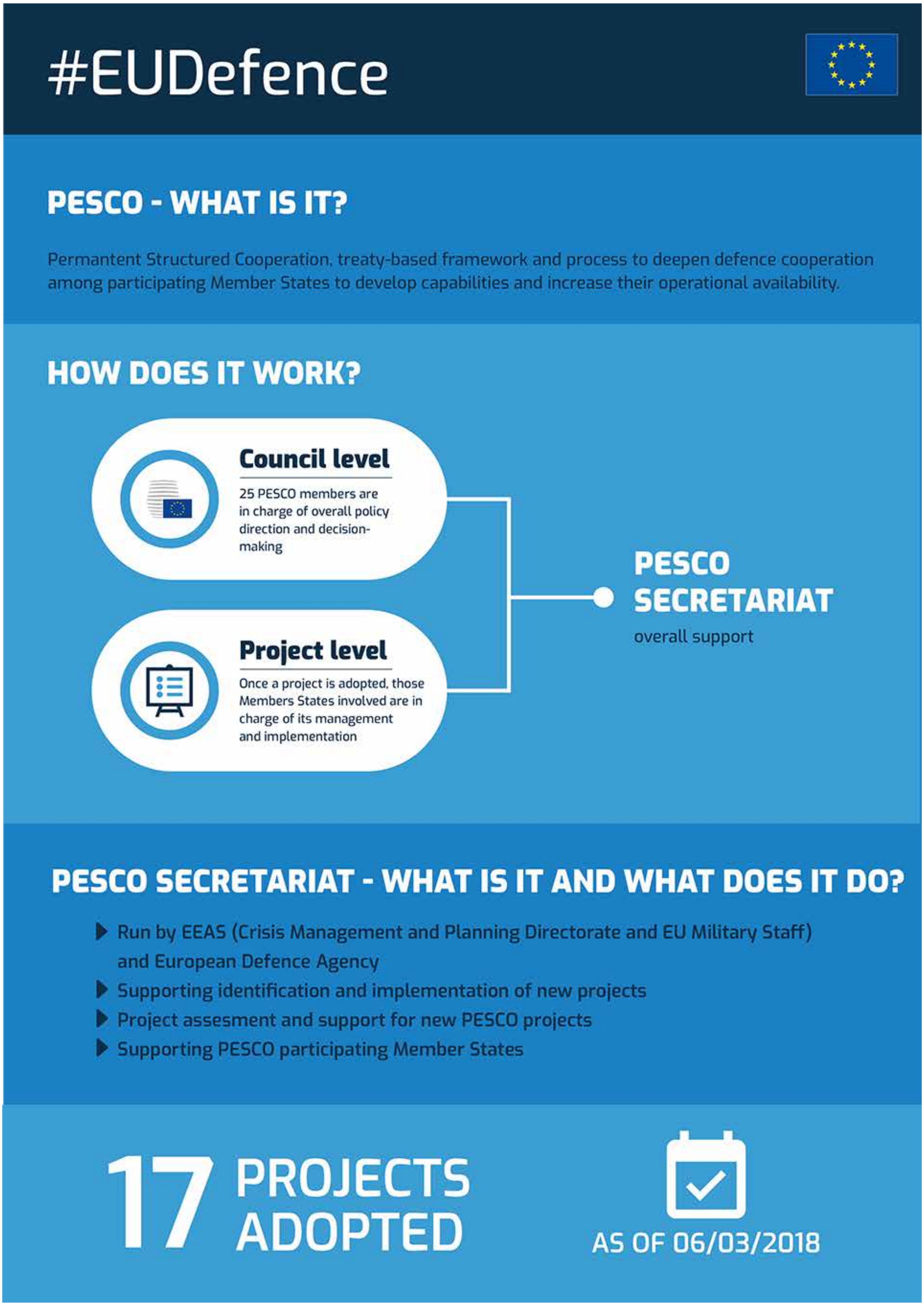
Cyber defence and CSDP

When it comes to cyber defence, the EU's evolution in the field is both more recent and also more limited, due to NATO's activities and the greater reticence of Member States to cooperate in a field in which stakes are considerably higher. The first relevant incursion of the EU into the field came in late 2012 with the approval of the Concept for Cyber Defence for EU-led CSDP operations. This was shortly followed by the EU defence ministers' agreement to put cyber defence on the Pooling & Sharing agenda. The European Defence Agency (EDA) has had a leading role in this field, facilitating and supporting Members States' related activities.

In greater depth, and in line with the above-mentioned 2013 Cybersecurity Strategy, the Council approved the Cyber Defence Policy Framework in November 2014, defining the general guidelines for the EU's activities in its external dimension, including CSDP, protection of the EEAS networks and relations with other partners, such as NATO.

In 2016, the EU and NATO reached an agreement on the issue – the Cyber Defence Pledge. This document focuses on areas of common interest such as fostering joint training exercises and deepening cooperation between states and between the two organisations. The European Commission also included cyber defence as a top priority in its European Defence Action Plan (November 2016). That has also been translated in two separate projects within the Permanent Structured Cooperation (PESCO): one on the creation of a European Cyber Information Sharing Platform and another on the development of European Cyber Rapid Response Teams.

Despite the EU's recent emphasis on resilience and deterrence – made clear by the 2017 Joint Communication by the European Commission and the High Representative for Foreign Affairs and Security Policy – its own role in terms of cyber resilience and cyber deterrence remains limited.



#EUDefence

PESCO - WHAT IS IT?

Permantent Structured Cooperation, treaty-based framework and process to deepen defence cooperation among participating Member States to develop capabilities and increase their operational availability.

HOW DOES IT WORK?

Council level

25 PESCO members are in charge of overall policy direction and decision-making

Project level

Once a project is adopted, those Members States involved are in charge of its management and implementation

PESCO SECRETARIAT

overall support

PESCO SECRETARIAT - WHAT IS IT AND WHAT DOES IT DO?

- Run by EEAS (Crisis Management and Planning Directorate and EU Military Staff) and European Defence Agency
- Supporting identification and implementation of new projects
- Project assesment and support for new PESCO projects
- Supporting PESCO participating Member States

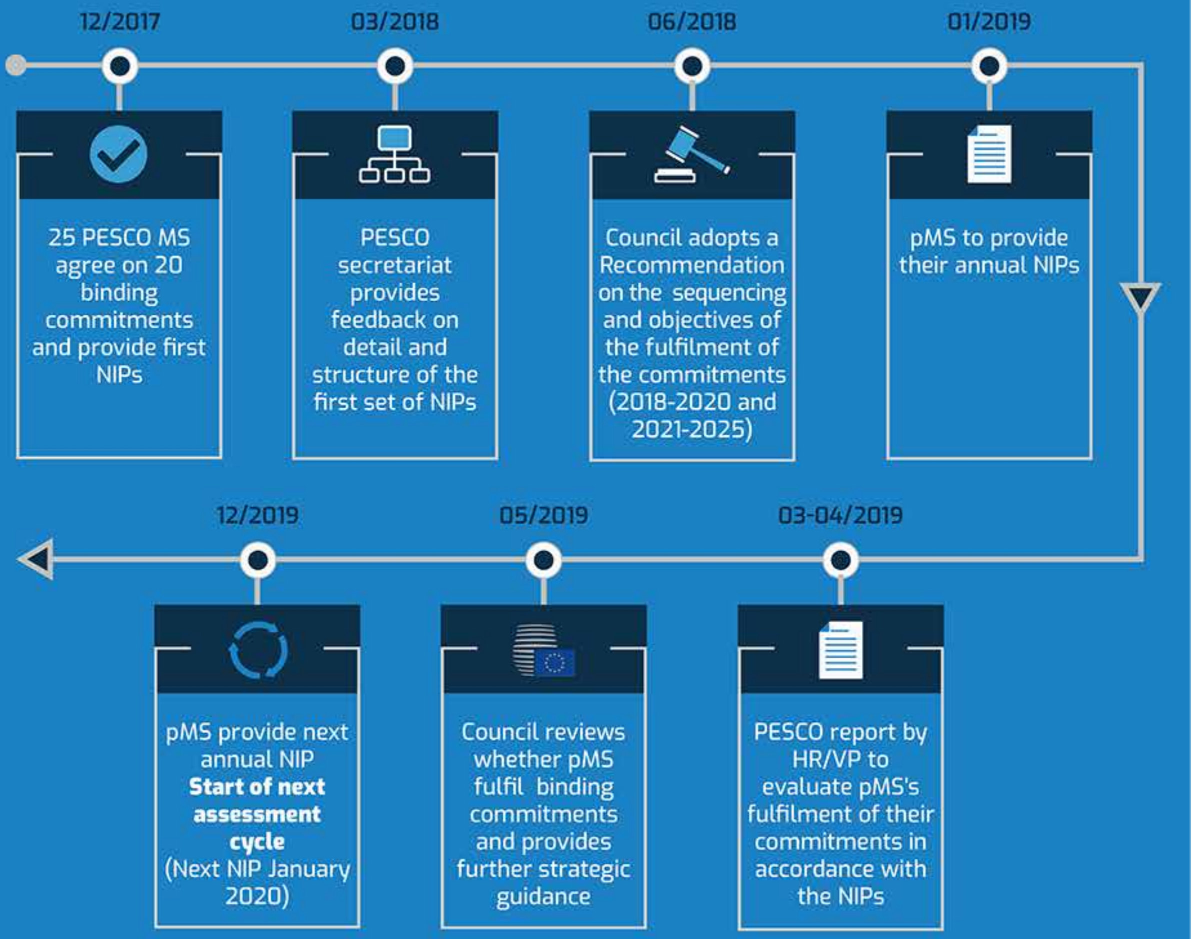
17 PROJECTS ADOPTED

AS OF 06/03/2018

#EUDefence

PESCO
ASSESSMENT PROCESS 12/2017 – 12/2019

HOW DOES IT WORK?



12/2017

25 PESCO MS agree on 20 binding commitments and provide first NIPs

03/2018

PESCO secretariat provides feedback on detail and structure of the first set of NIPs

06/2018

Council adopts a Recommendation on the sequencing and objectives of the fulfilment of the commitments (2018-2020 and 2021-2025)

01/2019

pMS to provide their annual NIPs

03-04/2019

PESCO report by HR/VP to evaluate pMS's fulfilment of their commitments in accordance with the NIPs

05/2019

Council reviews whether pMS fulfil binding commitments and provides further strategic guidance

12/2019

pMS provide next annual NIP **Start of next assessment cycle** (Next NIP January 2020)

PESCO = Permanent Structured Cooperation

MS = EU Member States

pMS = participating PESCO Member States

HR/VP = High Representative of the Union for Foreign Affairs and Security Policy / Vice-President of the Commission

EEAS = European External Action Service

EDA = European Defence Agency

NIP = National Implementation Plan

Council Recommendation = a non-binding legal act agreed on by the Council

Council Decision = binding legal acts agreed on by the Council

Conclusion

The EU cannot be considered a major cybersecurity actor yet, but it has considerably raised its interest and role in cyberspace over the past two decades, establishing itself as a focal point and facilitator for its Members States and, to a lesser extent, as a partner for third countries. The EU's future actorness in this field will be partly shaped by the more general developments of the EU as a diplomatic and security actor. However, in light of the strategic importance of the issue, it is unlikely that there will be a waning of interest or ambition in this domain.