EU Policy Brief

MARCH 2020 Issue #3

Centre for European Studies

EU Cyber Defense

Didier Danet, Stéphane Taillat, & Julien Nocetti, Military Academy of Saint-Cyr

Summary

* *Facing growing strategic and geopolitical challenges, the EU and its Member States have tried to devise a coordinated cyber defence policy. Like other defence and military policies, it builds on a diverse repertoire of cooperation. EU cyber defence often takes the form of "minilateral" cooperation, but also builds on frameworks devised in the NATO-EU relationship.*

Background/Challenge

- In light of a "return to great powers competition", Europe has become a battlefield between the US' and China's quest for technological, economic and strategic dominance. The EU's strategic and diplomatic agency and its ability to ensure its security have become matters of utmost importance.
- Most of the political debate in the EU addresses the issue of "digital sovereignty", as outlined in European Commission President von der Leyen's political guidelines as well as in several recent declarations by European head of states, most notably France and Germany.
- Growing concerns about Russia's geopolitical goals and US foreign policy—treating the EU as a trade rival and European allies within NATO as "free riders"—have led some European leaders to commit to further structure and reinforce their military and defense cooperation, including in cyberspace. These moves respond in particular to the current review of US strategic and military commitment to Europe, which resurrects European NATO members' dilemma between fears of entrapment and fears of abandonment.
- The deployment of 5G networks is taking place in a global cybersecurity threat landscape, notably characterized by an increase in supply-chain attacks. Overall, threats considered most relevant are the main traditional categories of cyber-related threats, which are tied to the compromise of confidentiality, availability, and integrity.

KEY FINDINGS

◊ "[G]rasping the **opportunities from the digital age** within safe and ethical boundaries" was one of the priorities identified by Commission President von der Leyen in her political guidelines. This ambition is in line with the position taken by former High Representative Federica Mogherini, who stated: "I am convinced that... the opportunities of global connectivity outnumber its dangers by far." However, in order to benefit from the advantages of digital transformation, it is necessary to deal with threats and attacks in the cyber realm.

◊ Within the global domain of cybersecurity, **cyber defense** is the set of activities carried out by the armed forces in cyberspace. It aims at protecting the proper functioning of information systems within the government and enabling armed forces to conduct their missions in the digital and the kinetic world. It encompasses defensive and offensive operations.

◊ The main features of the cyber domain — interdependence, transnationalism, and ambiguity —create **common challenges for doctrine, policy, and capability development of all EU Member States**. Even if cyber defense is a key prerogative of the Member States, collective initiatives are required. However, EU Member States do not fully share the same political vision of European strategic autonomy and military operations. Cooperation is also made more difficult because of the Member States' different maturity as far as Military Cyber Organizations are concerned.

◊ Because most European countries are part of the **EU and NATO**, collaborative efforts are undertaken within these two frameworks. Cyber defense is part of NATO's core task of collective defense. In 2016, Allies reaffirmed NATO's defensive mandate and recognized cyberspace as a domain of operations.

KEY FINDINGS (continued)

- As in other domains of military and defense cooperation, EU Member States could rely on **“minilateralism”**—ad hoc frameworks with a limited number of participants, dealing with specific issues—to structure their coordination and to enhance their technical, organizational and operational capabilities. Permanent structured cooperation (PESCO) could provide a model for governments that are willing and able to go further in establishing capabilities.
- As underlined by the **EU Cyber Defense Policy Framework** (2018), the EU’s approach is less operational from a military point of view, but much broader and holistic in its scope and ambition. It includes all major areas of EU competence. Different policy instruments are mobilized at the EU level, including market policy (Digital Single Market), foreign policy (Cyber Diplomacy), research funding (Horizon 2020), as well as law and regulation (Network and Information Systems Directive, General Data Protection Regulation).
- In addition, the EU has, since 2013, conceived and implemented an impressive set of policies, institutions and legislations in order to **coordinate the Member States’ cyber policies** and to create a shared culture of cybersecurity among them.
- A dramatic and significant example of the **EU being trapped in the technological war between the US and China** is its rejection of the US’ demand to ban Huawei from European 5G networks. This decision does not mean that the EU considers Huawei as a trustful partner. The real meaning of the EU Toolbox for 5G Security is that no provider should be chosen without a deeper risk assessment and mitigation procedure lead by a national information security agency. European telecoms companies who want to deal with Huawei are warned that, because the risk is higher due to the special relationship between the company and the Beijing regime, the mitigation measures must be appropriate and proportionate. This subtle balance does not close the European market to Huawei but it does not exclude restrictive measures if national security is threatened.

Policy Implications

- The mere possibility of autonomous European capabilities, whether as a “pillar” in NATO or in the EU framework, resurrects the debate about the risks of duplication vs. the importance of strategic autonomy to tackle challenges in case of US disinterest.
- Politically, an EU cyber defense policy framework ought to remain pragmatic. Operationally, the nagging question is that of the EU’s ability to act independently from the US. On the one hand, the current US approach raises concerns among allies. On the other hand, even the most advanced Member States are no match for unique US capabilities in terms of intelligence collection, disruptive operations, and manpower.
- Within NATO and the Five Eyes, Canada is in a similar situation as the UK. It is difficult to say “no” to the American neighbor even if a market-sharing solution between several operators, including Chinese companies, would be more efficient economically and technically, which does not preclude to give the latter a limited role taking into account national security imperatives.

Further Reading

- Carrapico, Helena, & Barrinha, André. “The EU as a coherent (cyber) security actor?”, *Journal of Common Market Studies*, 55(6), 2019, pp. 1254–1272.
- Wessel, Ramses. “Cybersecurity in the European Union: Resilience through Regulation?”, in Elena Conde, Zhaklin Yaneva, Marzia Scopelliti (eds), *Routledge Handbook of EU Security Law and Policy*, Routledge, 2019, pp. 283-300.

Author Information

- Didier Danet, Stéphane Taillat, and Julien Nocetti are researchers at the Military Academy of Saint-Cyr (France).
- Email: didier.danet@st-cyr.terre-net.defense.gouv.fr

Contact

- **Email:** ces@carleton.ca
- **Phone:** (613) 520-2600, Ext. 1087
- **Website:** www.carleton.ca/ces

With the support of the Erasmus+ Programme of the European Union

The Jean Monnet Centre of Excellence at Carleton University is supported by the Erasmus+ Programme of the European Union. The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.