Strategic Sectors | **Security & Politics**

EU Cybersecurity Capacity Building in the Mediterranean and the Middle East

Erwan Lannon
Professor
Ghent University

Cyberthreats on the Rise

The 2008 Report on the implementation of the European Security Strategy included "cybersecurity" for the first time among the priorities of the EU's external action, stating that: "modern economies are heavily reliant on critical infrastructure including transport, communication and power supplies, but also the Internet." If the EU Strategy for a Secure Information Society, adopted two years before, already addressed "cybercrime," the proliferation of cyber-attacks "against private or government IT systems" gave the spread of cyber-capabilities a "new dimension, as a potential new economic, political and military weapon."[1]

An EU Cybersecurity Strategy was adopted in 2013[2] followed, in 2016, by a first EU "Directive on Security of Network and Information Systems," known as the "NIS Directive,"[3] which harmonized the EU Member States' legislations. The EU thus created a political and legal framework for tackling this issue. As explained by Elaine Fahey, the EU Council put forward the concept of "cybercrime," alongside "cybersecurity," to also focus on the "regulatory process" for achieving "cyber resilience," and in order to link the EU's strategy with the Council of Europe's "Budapest Convention" (n° 185) on "cybercrime."[4]

The external dimension of this internal strategy developed almost simultaneously. At the security level, international cooperation is conducted with NATO allies, neighbours and partners,[5] notably in terms of joint exercises and training.[6] In 2017, the EU also had "cyber dialogues" with the US, China, Japan, the Republic of Korea and India.[7]

In 2018-19, the EU's approach in the Mediterranean in terms of cybersecurity has mainly been based on the priorities adopted in 2015 for the mid-term review of the European Neighbourhood Policy (ENP), which reinforced its security dimension, reflecting the priorities of the EU's 2016 Global Strategy on Foreign and Security Policy (EUGS[8]). The adoption in 2018 of the "EU Cybersecurity Act" is another important step, of specific interest for some Mediterranean Partner Countries (MPCs).

[1] EU Council, *Report on the Implementation of the European Security Strategy - Providing Security in a Changing World*, Brussels, 11 December 2008, S407/08, p. 5.
[2] European Commission and High Representative Joint Communication, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7 February 2013, JOIN (2013) 1 final.
[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, EU OJ L 194, 19 July 2016, pp. 1-30.
[4] Fahey, Elaine, "The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security," *European Journal of Risk Regulation*, Vol. 1/2014 pp. 46-61.
[5] See Lété, Bruno, "EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions" *GMF Policy Brief*, 15 December, 2017 www.gmfus.org/publications/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions.
[6] NATO's Mediterranean Dialogue was initiated in 1994 and "currently involves seven non-NATO countries of the Mediterranean region: Algeria, Egypt, Israel, Jordan, Mauritania, Morocco and Tunisia," www.nato.int/cps/en/natohq/topics_60021.htm?.
[7] Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU," Brussels, 13 September 2017, JOIN/2017/0450 final.
[8] Global Strategy for the EU's Foreign And Security Policy, June 2016 http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

The External Impact of the Development of the EU's Cybercapacities

As mentioned in the 2016 EUGS, at the internal level the EU increases its focus on cyber security "equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace."

The EU is now developing a "Cyber Diplomacy Toolbox" designed to respond to attacks through sanctions, international cooperation, dialogue, capacity building, joint investigations, etc.

The December 2018 Cybersecurity Act first reinforced the mandate of the EU Network and Information Security Agency (ENISA[9]), the "EU Agency for Cybersecurity," to better support Member States in tackling cybersecurity threats and attacks,[10] while contributing to the development of a "culture of NIS in society."[11] Secondly, it created an "EU framework for cybersecurity certification" for "products, processes and services" that will be "valid throughout the EU." It is, therefore, internal market legislation,[12] meaning that the Commission, which is in charge of the digital single market initiative, will promote cooperation among Member States and is also responsible for "research and industrial collaboration" and "certification of digital products and services to ensure safe use."[13] This is therefore important for MPCs like Tunisia or Morocco, which may reach Deep and Comprehensive Free Trade Agreements. The possibility that ENISA offers for MPCs to participate in EU programmes and agencies, with conditions and on a case-by-case basis, is also worth highlighting.

Also of importance in terms of defence, is that the 2017 first Permanent Structured Cooperation (PESCO), concerning common security and defence policy, included, as of March 2018, projects related to "Cyber Threats," an "Incident Response Information Sharing Platform," "Cyber Rapid Response Teams" and "Mutual Assistance in Cyber Security."[14]

Reinforcing the EU's "Cyber Diplomacy Toolbox"

At the external level, the 2016 EUGS stressed the need for the EU to enhance its cybersecurity cooperation with "core partners such as the US and NATO" and to develop a "common cyber security culture."[15] The reference to the US and NATO is of crucial importance given the "collective defence" assistance clause of the Washington Treaty.[16] In this regard, NATO's "very first Cyber Defence Policy" was adopted in 2008. Eight years later, an EU-NATO Joint declaration emphasized the need to help "neighbours and partners" to build a "defence and security capacity" and foster their "resilience" in the "East and South."[17]

[9] See: www.enisa.europa.eu and European Commission, EU negotiators agree on strengthening Europe's cybersecurity, December 2018, https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en11.

[10] ENISA was set up to help reach a "high level of network and information security (NIS)" within the EU, including cybersecurity exercises and strategies, and data protection issues. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, EU OJ L 77, 13 March 2004, p. 1.

[11] ENISA, June 2019, www.enisa.europa.eu/about-enisa.

[12] European Commission, EU negotiators agree on strengthening Europe's cybersecurity, *op. cit.*

[13] EU ISS, Estonian Presidency of the Council, Hybrid threats and the EU - State of play and future progress, Conference Report, 2017, www.iss.europa.eu/sites/default/files/EUISSFiles/EE%20hybrid%20event%20report.pdf.

[14] EU Council, Updated list of PESCO projects, 19 November 2018, www.consilium.europa.eu/media/37028/table-pesco-projects.pdf.

[15] *Op. cit.,* pp. 21-22.

[16] On the potential invocation of Article 5 see: Missiroli, Antonio, "The Cyberhouse Rules: Resilience, Deterrence and Defence in Cyberspace," *ISPI Commentary*, 2 March 2018, www.ispionline.it/it/pubblicazione/cyberhouse-rules-resilience-deterrence-and-defence-cyberspace-20378.

[17] EU-NATO Joint Declaration adopted by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, Press Release (2016) 119, Warsaw, 8 July 2016, www.nato.int/cps/en/natohq/official_texts_133163.htm.

Furthermore, the EU is now developing a "Cyber Diplomacy Toolbox" designed to respond to attacks through sanctions, international cooperation, dialogue, capacity building, joint investigations, etc. In June 2017, the EU Council stressed that all the EU's "diplomatic efforts should aim, as a matter of priority, to promote security and stability in cyber-

"EU Cyber Capacity Building guidelines" are to be developed for "better political guidance and prioritization of EU efforts in assisting the third countries." Indeed, some Mediterranean partners lack proper cyber defence capabilities and their infrastructures are vulnerable

space through increased international cooperation" and that Common Foreign and Security Policy measures "including, if necessary, restrictive measures," are "suitable for a Framework for a joint EU diplomatic response to malicious cyber activities." At the same time, the EU should "encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term." The EU Council then urged Member States to "give full effect to the development of a Framework for a joint EU diplomatic response to malicious cyber activities."[18] The 2017 Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[19] therefore introduced a specific point on the "strengthening of international cooperation on cybersecurity" referring, among the priorities, to:

— the development of "regional confidence-building measures";
— ensuring that cybersecurity "does not become a pretext for market protection and the limitation of fundamental rights and freedoms, including the freedom of expression and access to information";
— "modernizing EU export controls, including the introduction of export controls on critical cyber-surveillance technologies that could cause human rights violations or be misused against the EU's own security, and stepping up dialogues with third countries to promote global convergence and responsible behaviour in this area."

This last priority is of specific interest for relationships between some Member States and MPCs.[20]

The EU's Cybersecurity Capacity Building in the Mediterranean and the Middle East

The 2017 Joint Communication included in its key actions, supporting "third countries' ability to address cyberthreats." It is clearly stated that the priorities for capacity-building will be the "EU's neighbourhood and developing countries experiencing fast growing connectivity and rapid development of threats." In this regard, a dedicated "EU Cyber Capacity Building Network should be set up, bringing together the EEAS, Member States' cyber authorities, EU agencies, Commission services, academia and civil society." Moreover; "EU Cyber Capacity Building guidelines" are to be developed for "better political guidance and prioritization of EU efforts in assisting the third countries." Indeed, some Mediterranean partners lack proper cyber defence capabilities and their infrastructures are vulnerable. As an example of the growing cyberthreats, we could recall a cyberattack called "Triton," named after a malware. The latter was developed to "manipulate Schneider Electric's Triconex Safety Instrumented System (SIS) control systems - emergency shutdown systems - and was discovered on the network of a critical infrastructure operator in the Middle East." Specialized reports pointed out that the

[18] EU Council, Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), Brussels 7 June 2017.
[19] Brussels, 13 September 2017, JOIN(2017) 450 final.
[20] For a recent example see: FIDH, Egypt: a repression made in France: Exports of Weapons and Surveillance Technologies, Report n°716a, 2 July 2018, www.fidh.org/en/issues/litigation/egypt-a-repression-made-in-france.

"group of pirates behind Triton - suspected of links with Russia - remains active."[21]

It is therefore no surprise that, among the seven main priority areas devoted to security in the November 2015 Joint Communication on the mid-term review of the ENP, "fighting cybercrime" is in a good position.[22] That also means that, beyond cybersecurity, a focus on legislation approximation or at least regulatory convergence is included in cooperation with ENP partners.

Cyberthreats are like environmental issues: they do not take into consideration political borders, as they are by nature transnational and transregional

On a security level, new programmes and actions have also been launched. The 2018 report on Euro-Jordanian relations stressed, for example, that the EU programme on the fight against violent extremism had been finalized, and that several projects had been implemented in the framework of sectors like "crisis management," or "capacity building of public security." Projects like the "EU/MENA Counter-Terrorism Training Partnership 2 (CEPOL CT 2)" and the old Euromed Justice ("ICSP CT Mena ENI EUROMED Justice IV") and Police programmes were mentioned together with "CyberSouth" ("Cooperation on cybercrime in the Southern Neighbourhood"), which is a joint project of the EU and the Council of Europe[23] aimed at strengthening "legislation and institutional capacities on cybercrime and electronic evidence" in the Southern Neighbourhood, "in line with human rights and rule of law requirements." The "initial priority areas" are: Algeria, Jordan, Lebanon, Morocco and Tunisia, and the project focuses on "legislation; specialized services and interagency, as well as public/private cooperation; judicial training; international cooperation" and "strategic priorities on cybercrime and electronic evidence."[24]

Another example is that the EU and Lebanon have developed an "Action Plan to enhance the cyber security capabilities of internal security forces." This is part of a "Regional Development Agenda" titled "CT MENA Counter-Terrorism in the Middle East and North Africa" (2017-2020)[25]. It is aimed at developing "criminal justice capacity" to counter terrorism "across intelligence, law enforcement and criminal justice components under the rule of law." This is achieved through institutional capacity, "coordination and cooperation" and expertise.[26] Nine members of the Arab League are currently involved.[27]

Conclusion

Cyberthreats are like environmental issues: they do not take into consideration political borders, as they are by nature transnational and transregional. As stated during the preparation of a cyber exercise for European defence ministers in 2017[28]: "As the cybersphere doesn't discriminate, the number of potential targets is equivalent to the number of systems and their access points used."[29] Cybersecurity is becoming a major sector for cooperation, not only in

[21] ZDNet, *Cybersécurité: les principales leçons de la cyberattaque Triton*, 3 May 2019, www.zdnet.fr/actualites/cybersecurite-les-principales-lecons-de-la-cyberattaque-triton-39884243.htm.

[22] The other six being: Security sector reform; Tackling terrorism and preventing radicalization; Disrupting organized crime; Chemical, Biological, Radiological and Nuclear Risk Mitigation; Common Security and Defence Policy; and Crisis management and response. Joint Communication: Review of the European Neighbourhood Policy, Brussels, 18 November 2015, JOIN (2015) 50 final.

[23] Joint Staff Working Document, Report on EU-Jordan relations in the framework of the revised ENP (2017-2018), SWD (2018) 485 final, 29 November 2018, p. 3.

[24] See: www.coe.int/en/web/cybercrime/cybersouth.

[25] European Commission and High Representative, Report on EU-Lebanon relations in the framework of the revised ENP (2017-2018), SWD(2018) 484 final, 29 November 2018, p. 3.

[26] See: http://ct-morse.eu/projects/.

[27] Algeria, Egypt, Iraq, Jordan, Lebanon, Libya, Morocco, Palestine, Syria and Tunisia.

[28] ENISA. "European defence ministers meet for cyber exercise supported by ENISA," 8 September 2017, https://www.enisa.europa.eu/news/enisa-news/european-defence-ministers-meet-for-cyber-exercise-supported-by-enisa.

[29] EU presidency, "Estonia stages cybersecurity exercise for EU defense ministers," 7 September 2017 https://news.err.ee/617176/estonia-stages-cybersecurity-exercise-for-eu-defense-ministers.

financial or trade terms, but also as an indicator of the depth of the political/security relation and trust between partners. In the Mediterranean it is already a major issue, as demonstrated by the electronic war being waged in Syria. As underlined by Edwin Grohe, the "cyber element of the Syrian civil war has had a more important role than one might have expected," and we "will observe a constant cyber 'arms race' in which nation-states try to increase their capabilities of cyber-attack, exploitation and espionage, as well as their cybersecurity capability to defend against those very same operations."[30]

Although approximating legislation on cybercrime at the pan-euro level is indispensable, it is currently not sufficient. Given the rise of cyberthreats, there is a need for a "Pan-Euro-Mediterranean Cybersecurity Strategy" (or "PEMCS"), not only for the public sector and critical infrastructures,[31] but also to help economic operators facing growing challenges in terms of cyberthreats. Research and technological tools are also of crucial importance.[32]

Cybersecurity is becoming a major sector for cooperation, not only in financial or trade terms, but also as an indicator of the depth of the political/security relation and trust between partners

The adoption, in 2018, of the EU Cybersecurity Act[33] is of specific interest for the MPCs as it also includes an article 42 related to "Cooperation with third countries and international organizations," which states that ENISA "may establish working arrangements with the authorities of third countries and international organizations." Even if these arrangements "shall not create legal obligations incumbent on the Union and its Member States," it is an opportunity not to be missed by some Mediterranean Partner Countries.

[30] Grohe, Edwin. The Cyber Dimensions of the Syrian Civil War, Implications for Future Conflict, 2015, Johns Hopkins University Applied Physics Laboratory LLC, https://apps.dtic.mil/dtic/tr/fulltext/u2/a620195.pdf.

[31] See: Cassotta, Sandra et al., "Cyber Threats, Harsh Environment and the European High North (EHN) in a Human Security and Multi-level Regulatory Global Dimension: Which Framework Applicable to Critical Infrastructures under "Exceptionally Critical Infrastructure Conditions" (ECIC)?", 2019, In Beijing Law Review (BLR), Special Issue 12, at press.

[32] In this regard, a "public-private partnership for cybersecurity industrial research and innovation" between the EU, represented by the European Commission and the European Cyber Security Organization (ECSO) association was concluded a few years ago. See the European Commission's decision of 5 July 2016 on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organization, Brussels, 5 July 2016, C(2016) 4400 final.

[33] The Act has been adopted but not yet published in the EU's Official Journal, see: www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.html?redirect#BKMD-20.