The Europe of digital security: Very legalistic, hardly technological, insufficiently economic

Nicolas Arpagian, scientific director of Digital Security at the Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ)

For: In Jean-Pierre Dardayrol (ed.) *The European digital union* [special issue of *Réalités Industrielles*, August 2016]

Summary:
Although Europe claims, rightly so, to have a knowledge-based economy and solid resources for creating economic value, it is not at all in the lead on digital security. Most of its output in this domain has been texts (EU directives and regulations) with obligations about the security of the information industry's infrastructure. Since the 28 member states have not managed to create the conditions for a global player in cybersecurity to emerge, the fight against cybercriminality is mainly undertaken by national police forces. The EU Agency for Network and Information Security (ENISA) is still struggling to sustain its financing for the coming years. Since member states are using digital technology to defend their own strategic interests (the security of vital operators, collection of economic or diplomatic information, etc.), they are reluctant to endow Europe with the integrated, effective tools that would force recognition from the big powers in the digital world (the United States, China and Russia).

As the history of the construction of the European Union attests, the Old World seems more capable of building an economic and juridic alliance than of becoming a front-rank political or military player.[1] A source of apprehension for the future is that Europe has, thanks to its purchasing power, so quickly adopted all the latest, state-of-the-art digital equipment and fittings (for high-speed connections, cloud computing, e-business, social media, smartphones…) but without securing its own autonomy.

Europeans are customers of the big on-line platforms (in particular, the GAFAM: Google, Apple, Facebook, Amazon and Microsoft) but have been incapable of proposing genuine alternatives of European origin. These multinational firms carry so much weight that they can impose the general conditions for using their services. They have unilaterally designed the conditions and, too, update them when they want — without having to go through any real negotiations. These contracts, usually written in English, very often require the referral of litigation to the American court system. They now form the legal framework of the planetary Internet.

Despite its economic might, legal expertise and purportedly strong position associated with its status as a client, Europe, for sure, does not hold the place it should have in the digital realm. This situation is very probably the outcome of the 1970s and 1980s, when Old World elites did not take seriously the potential of information technology. For example, the measures adopted on computer technology after Valéry Giscard d'Estaing was elected president of France in 1974 led to a

[1] The views expressed in this article are the author's own. This article has been translated from French by Noal Mellott (Omaha Beach, France).

sharp reduction of the budget for investments in telecommunication networks and packet switching, in particular the Cyclades computer network.[2]

European digital security… designed by national authorities!

Europe has not approached cybersecurity in the most operational way possible. The European Network and Information Security Agency (ENISA) was set up in 2004.[3] But its low budget (ten billion euros annually), the localization of its headquarters in Crete (far from decision-making centers) and its limited political mandate do not allow for working out a truly mutual approach to digital security. According to a warning in March 2016 from its German director, Udo Helmbrecht, the agency, saddled with debts, did not even "*have the funds to hire cybersecurity experts to work on the Internet of Things, the increase of devices with internet connections, and only had two experts on cloud computing.*"[4] ENISA has to beg for additional funds just to maintain its activities and pay the rent — hardly an incentive for the best specialists to apply for a job at the agency.

Having persisted for more than a decade, this situation is evidence of member states preserving their own resources and expertise in matters of cybersecurity. Chancelleries do not imagine pooling know-how at the EU level, neither in the field of defense nor in the fight against cyberattacks.

A depressing European oddity

Europe still has world champions in the automobile or pharmaceutical industries, but has clearly neglected the digital realm. American platforms have found the Old World to be a very suitable place for expanding their business given that consumers there are numerous, solvable and fond of new technology. Furthermore, the platforms can, given disparate national laws on the continent, make countries compete with each other to become the place where these multinational firms will install their European headquarters.

Meanwhile, countries such as China or Russia have proven capable of setting up their own social networks, their own instant messaging systems, their own e-businesses. They even have their own specialists in cybersecurity.

In Europe, only the Czech Republic (ten million inhabitants) has its own national leader, Seznam.[5] As the first search engine used by Czechs, it has kept Google at bay. Local firms are not missing in action because they have been technological fatalities. Indeed, it is the freedom of cybernauts as consumers to choose that has allowed for the emergence of players in the digital realm. The fit between demand and the services provided is still the best way to attract users and make them loyal — users who seldom adopt nationality as the criterion for determining their browsing choices.

The EU is known for is capacity to make rules and regulations, and it has already adopted several legal texts on cybersecurity. EU directive 2013/40 seeks to harmonize member states' penal legislation about attacks and infringements on information systems.[6] The very title of a joint

[2] See the interview with Louis Pouzin in *Revue de La Société de l'électricité, de l'électronique et des technologies de l'information et de la communication*, REE N°4/2013, 81. Available at:
https://www.see.asso.fr/node/5217/file_preview/file_text_text

[3] ENISA website: www.enisa.europa.eu

[4] Cathérine Supp, "Cash-strapped EU cybersecurity agency battles Greece to close expensive second office", *Euractiv*, 25 March 2016. Available at:
http://www.euractiv.com/section/digital/news/cash-strapped-eu-cybersecurity-agency-battles-greece-to-close-expensive-second-office/

[5] Seznam website: www.seznam.cz

[6] "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems". Available at:
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013L0040&from=EN

communication by EU authorities quite clearly sums up the paradox of the approach adopted by 28 member states: "Cybersecurity strategy of the European Union: An open, safe and secure cyberspace".[7] Experts on cybersecurity usually consider the adjectives "open", "safe" and "secure" to be incompatible!

Whereas the United States has the well-known Federal Bureau of Investigation (FBI) for policing 320 million Americans, there is no similar service of domestic security for 510 million Europeans. In response to the international scope of cybercriminality, Europol opened a European Cybercrime Center (EC3) in the Hague in 2013.[8] This center has the assignment of facilitating exchanges of information and good practices. It is a point of contact for national police forces, but it is not at all an integrated security force for launching its own actions anywhere in the EU.

Mafias of all sorts revel in digital mobility and keep up their sleeve the ace of penal impunity — the possibility of jumping across borders. Nonetheless, the forces defending law and order mostly operate under national laws and legal procedures.

A skeletal European cyberdefense

Although government websites often pass information on a diplomatic, reserved tone, a comment on European cyberdefense that leaves little room for any reservations was posted on 10 August 2011 on the French Defense Ministry's official website: "*Despite mentioning cyber issues in its official texts and setting up structures and activities devoted to them, the European Union is lagging, compared with another alliance, NATO. In fact, there is little cooperation.*"[9] The fault is not a lack of discussion of the topic, which has figured on the agendas of special conferences and scientific meetings.

For more than a decade now, European diplomats seem to want to make a break with the regrettable situation that resulted from the signature in 1952 of a treaty for the creation of a European Defense Community (EDC): two years later, the French National Assembly refused to ratify the treaty. This refusal has left a lasting mark on public opinion, namely: the fear lest an army at the European level undermine national independence.

When reading government documents from the early 21st century, we notice that mentalities have evolved. There is now a glimmer of hope for making advances on this issue. On the aforementioned web page of the Ministry of Defense, we read, "*According to the report from the Defense Commission on Information Warfare, submitted in 2008 to the European Security and Defense Assembly, the European Defense Agency (EDA) should implement a doctrine of European cyberwarfare at the level of capacities and of research and technology.*" More than eight years later, we are still awaiting this doctrine; and the EU's Common Security and Defense Policy (CSDP) is still tepid with respect to both conventional and cyber warfare. This situation was summed up in a statement made by Vice-Admiral Arnaud Coustillière, cyberdefense officer, at a conference in December 2015: "A *European defense would be necessary before having a European cyberdefense.*"[10]

[7] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity strategy of the European Union: An open, safe and secure cyberspace", 7 July 2013. Available at: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=en

[8] European Cybercrime Center (EC3) at the Europol website: https://www.europol.europa.eu/ec3

[9] Nelly Moussou,"Union Européenne: La lente mise en place d'une cyberdéfense commune", 10 August 2011. Available at: http://www.defense.gouv.fr/portail-defense/enjeux2/cyberdefense/la-cyberdefense/bilan-et-evenements/2011-cyberdefense-enjeu-du-21e-siecle/international/voir-les-articles/union-europeenne-la-lente-mise-en-place-d-une-cyberdefense-commune

[10] Conference "L'intégration du cyber dans la planification des opérations et des missions de la Politique de Sécurité et de Défense Commune de l'Union européenne", conference organized by the Chaire Cyberdéfense et Cybersécurité, Saint-Cyr, on 3-4 December 2015 in Brussels.

The contrary interests of members of the European family were also exposed by the revelations in November 2015 that German intelligence services (BND) had intercepted, for the American administration, communications between members of the French government.[11] Political allies are still economic rivals. The principle, formulated by General de Gaulle, that a state does not have friends is more than ever actual.

The switch toward a digital society with systems for irrigating administrative and business organizations with information has blurred the boundary between defense and security. Since information can be captured unawares to senders or receivers, cyberdefense has a key place in the arsenals of the nations and, too, firms that now opt for the discretion of services from companies with no qualms about doing the digital dirty work. In cyberspace, there are no military parades for exhibiting the latest equipment and demonstrating force. Real power is guesswork; and silence is the rule as long as there is no indisputable proof of responsibility. On this theater of operations, Europe has reneged on allying its forces;[12] and each member state is acting on its own, in what might be an ultimate demonstration of declining sovereignty…

[11] "Laurent Fabius aurait été espionné par les services secrets allemands", *Le Monde*, 11 November 2015. Available athttp://www.lemonde.fr/europe/article/2015/11/11/laurent-fabius-aurait-ete-espionne-par-les-services-secrets-allemands_4807321_3214.html

[12] Nicolas Arpagian "Internet et la fiscalité vont imposer le fédéralisme à l'Europe", *Les Echos*, 19 August 2015. Available at: http://www.lesechos.fr/19/08/2015/LesEchos/22004-028-ECH_internet-et-la-fiscalite-vont-imposer-le-federalisme-a-l-europe.htm