ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
3 May 2018

THE FRENCH STRATEGIC REVIEW OF CYBER DEFENSE

François Delerue

IRSEM

Aude Géry

Rouen University

On 12 February 2018, the General Secretary for Defense and National Security Louis Gautier presented the French Strategic Review of Cyber Defense. The French approach to cyber defense in 2017 and 2018 has been pivotal. After the creation of the Cyber Defense Command (COMCYBER) within the Ministry of the Armed Forces in January 2017 the government published several key strategy documents: the Defense and National Security Strategic Review on 11 October 2017; theInternational Digital Strategy on 15 December 2017; thecyber defense Strategic Review on 12 February 2018; and the Military Planning Act 2019-2025, which will be published this coming summer and will contain provisions relating to French cyber defense strategy.

The Strategic Review of Cyber Defense has been portrayed by Louis Gautier and other French officials as a seminal document, comparable to the first French White Paper on Defense and National Security of 1972, which established France's nuclear doctrine. The Review reaffirms and further develops the French position on cyber defense, already expressed in previous documents and speeches, namely the 2013 White Paper on Defense and National Security; the speech given by Jean-Yves Le Drian, then Minister of Defense, during the visit of the DGA-MI, Bruz (Ille-et-Vilaine, France), 12 December 2016; the 2017 Defense and National Security Strategic Review; and the 2017 International Digital Strategy and the subsequent speech made by Jean-Yves Le Drian, Minister of Europe and Foreign Affairs, in Aix-en-Provence on 15 December 2017.

The Review is divided into three parts. The first part relates to the dangers of the cyber world. It analyzes the threat landscape, different models of cyber defense organization in the world and the evolution of international regulation of cyberspace. It highlights that although the last Group of Governmental Experts on Developments in the Field of Information and Tele-

François Delerue is a researcher in international law and cyberdefense at the Institute for Strategic Research (IRSEM – Institut de Recherche Stratégique de l'Ecole militaire) and an associate researcher at the Castex Chair of Cyberstrategy; Aude Géry is a Ph.D. candidate at Rouen University, working on international law and cyber weapons proliferation and an associate researcher at the Castex Chair of Cyberstrategy.

communications in the Context of International Security in the United Nations (UNGGE) failed to reach a consensus, it did not "in any way call into question the norms and principles agreed upon in previous years" (p.36). Finally, this first part reaffirms the French rejection of the concept of cyber deterrence, leaving it only for nuclear strategy.

The second part of the Review relates to "The State, responsible for the Nation's cyber defense". First, it recalls France's specific cyber defense organization model where offensive and defensive missions and capacities are strictly separated (p.45). It implies that authorities in charge of cyber protection are distinct from the ones conducting intelligence and offensive missions. The Review continues to detail cyber defense governance mechanisms, presents recommendations regarding the protection of critical infrastructures operators and identifies a new category of critical infrastructures called "supercritical infrastructures". This category refers to infrastructures that play a crucial role in supporting other critical infrastructures, meaning electronic communications and electronic energy providers (p.61). The Review then details France's strategy regarding its international action. It proposes a classification scheme for cyberattacks (p.79), similar, though not identical, to the Cyber Incident Severity Schema adopted by the United States, on which political authorities should rely to react during a crisis. According to this scheme, the gravity of a cyberattack would be evaluated against five main criteria and five complementary criteria. The review continues to outline France's approach to international law and its applicability to cyber operations. It must be noted that it is the first time France publishes such a detailed document on its use of international law. The document evokes that France has long held a position according to which international law applies to cyberspace and reaffirms that "its sovereignty over information and communication technologies infrastructures, persons and cyber activities located within its territory, subject to its legal obligations" (p.82). It details some of the States' international legal obligations in cyberspace such as the duty of due diligence, and possible responses under international law such as mechanisms of international cooperation and peaceful settlement of disputes as well as self-defense. It particularly insists on self-defense, explaining France's interpretation of article 51 of the United Nations Charter in cyberspace. The Review also affirms that France must continue to work towards a more open, safe, secure and stable cyberspace and promote norms of responsible behavior for both state and non-state actors. Following the Minister of European and Foreign Affairs Jean-Yves Le Drain's speech in conjunction with the UN General Assembly last October, the Review details the three propositions regarding the regulation of the private sector. First it calls for greater control of offensive action by the private sector, whether on their own behalf or on behalf of other non-state actors (p.88), leaving a possibility to do so when a State acts in self-defense (p.89). Second, it proposes to establish corporate responsibility in designing, deploying and maintaining digital products for systemic private actors. It specifies "this responsibility could translate into an obligation for systemic companies to guarantee long-term security for their products, in particular by providing adequate patching for vulnerabilities". This responsibility would be, according to the Review, an obligation of conduct, in opposition to an obligation of result. Finally, the Review presents propositions to fight cyber weapon proliferation. Two options are laid out. The first would be to promote a norm of responsible behavior by which States would commit to control the export of malicious cyber tools and techniques (p.104). The second would be to consider the inscription of certain software (those that are not only produced to punctually penetrate systems but to last in these systems or to damage their targets) to the list of munitions of the Wassenaar Arrangement (p.104).

The Review insists on the importance of international cooperation (pp. 90-91). Following the failure of the last UNGGE, the Review affirms that it does not end diplomatic efforts and that it calls to think over and redesign the ways these matters are dealt with at the UN level. The Review also lists other fora where these discussions are taking place at the multilateral level (G20, G7) and regional level (OSCE), and in which France is taking an active part. Alongside these inter-state debates, the Review underlines the importance of "track 2" fora, gathering states, civil society, private actors and researchers (e.g. the Global Commission on the Stability of Cyberspace, the Sino-European Cyber Dialogue, the Global Forum on Cyber Expertise, etc.). Finally, the Review recommends a French initiative at the G20 for the regulation of the activities of the private sector having an effect on the international security of cyberspace (p.91).

The third part of the Review, entitled "The state, responsible for the cybersecurity of society" is articulated around the concept of digital sovereignty, notably implying the necessity to take into account the security of the citizens, the private sector and local authorities when defining French cyber defense. Digital sovereignty is defined as the capacity of the State to act sovereignly in cyberspace by preserving its autonomous capacity of appreciation, decision and action, while simultaneously protecting the traditional components of sovereignty from the dangers arising from the increasing digitization of societies (p. 93). This last part describes the organization of the national cybersecurity and outlines the role of the French Cybersecurity Agency (ANSSI – Agence nationale de la sécurité des systèmes d'information). In conclusion, it is important to highlight that the Cyberdefense Strategic Review is also a seminal document as it is the first time that the various approaches and strategies of the different components of the State – including the Ministry of Foreign Affairs, Ministry of Defense, ANSSI, etc. – are gathered and articulated into one national strategy.