Regulations for private actors in cyberspace?

Florian Escudié,
Ministry of Europe and Foreign Affaires

Abstract:
As a new space for conflicts, digital technology confers on the private sector (in particular, certain systemic actors) a critical role and an unprecedented responsibility for peace-keeping and national security. Perceived till recently as the responsibility of nation-states alone, cybersecurity and a stable order in cyberspace are now widely perceived to be issues that directly concern private actors, whence a growing demand for clarifying their obligations. In November 2018, France launched a call for trust and security in cyberspace that identifies several axes for better regulating the role of private actors: fight against the proliferation of programs and techniques with criminal intent, increase the security of digital products and services, and forbid offensive actions undertaken by private actors and outlaw the use of mercenaries. Work is under way in various settings, for instance the OECD, to work out efficient regulations on this topic.

On 12 November 2018, the regulation of cyberspace reached a turning point, when France hosted two major events: the Paris Peace Forum and the Internet Governance Forum.[1] The president of France launched the "Paris Call for Trust and Security in Cyberspace".[2] At the time of writing, 69 nation-states, 361 firms and 149 NGOs have declared their support for this call, which has brought together for the first time quite different parties who make the commitment to work together to strengthen international norms and uphold and protect personal rights on line (as is already the case in the physical world). This "multi-actor" approach has led to setting several priorities: the prevention of criminal activities on line and resilience in handling them; the protection of accessibility to the Internet and of the Internet's integrity; the prevention of interference in elections; the fight against violations of intellectual property rights on line and against the proliferation of malicious programs and techniques in cyberspace; increased security for digital products and services; the promotion of "cyberhygiene"; and the prohibition of cybermercenaries and of the conduct of offensive actions by nongovernmental actors.

Security in cyberspace had previously been widely perceived as the responsibility of nation-states alone. For several supporters of the Paris Call however, the intent was not so much to recognize that the role traditionally assigned to states under international law should apply in cyberspace too. Many of them pointed out that states were developing digital tools and techniques for offensive purposes, sometimes outside any framework for upholding the law. The Snowden Affair and the revelation of cases of large-scale espionage crystalized preoccupations and criticisms. Emphasizing their responsibility toward their customers, several big high-tech firms stood in the

[1] This article, including quotations from French sources, has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in April 2020.

[2] Available via https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf.

front ranks of those who criticized such practices.[3] However they had nothing to say about their own responsibilities — even though most cyberattacks exploit flaws and points of vulnerability in the products and services they have developed.

The Paris Call is not intended to point a blaming finger but, instead, to look together for the means to ensure stability in cyberspace and protect activities there. Each supporter of the call has recognized its responsibilities and accepts that cyberspace should be fully under international law and under regulations adapted to the specific characteristics of this space. These are the grounds for eventually tightening the rules that govern the relations between governmental and nongovernmental actors in cyberspace.

Private entities hold a central position in this new zone of conflict.

The digital realm has become a space of conflict. The growth of digital technology has granted the private sector, in particular a few systemic entities, a critical role and unprecedented responsibility in keeping the peace and ensuring national security. This responsibility stems from the very nature of cyberspace and its construction by private entities. Among the weapons widely scattered over this "battlefield" are commercial products for the general public. Large-scale attacks exploit the defects of these products. NotPetya, for instance, took advantage of a flaw in M.E.DOC, a bookkeeping software, for the wave of attacks in June 2017. Given the increasing digitization of our societies, the attack surface is expanding as systems and equipment are ever more interconnected. The points of vulnerability in these products make it easier for hackers to assemble an important base for an attack, as happened in the autumn of 2016, when the Mirai malware turned thousands of connected devices with a low level of security into a giant fleet of botnets for massive distributed denial of service attacks (DDoS).

Whereas some firms might, notwithstanding their efforts and sometimes unknowingly (as in the film *Zero Days*), end up being a party to malevolent actions that exploit the flaws inherent in their products, other private entities actively take part in attempts at destabilization. For one thing, private firms produce some of the "weapons" (intrusive or destructive software) exchanged on this slightly regulated market. For another, mercenary services are thriving. To the victims of an attack, they make offers for offensive actions to break into a third party's information systems and retrieve stolen data. The actions proposed might even go so far as retaliation following a logic of legitimate defense ("hack back"), which has extremely destabilizing effects.

There is a growing demand for a clarification of the obligations of the nongovernmental parties active in cyberspace. This demand first came from states, who wanted to avoid any challenge to their monopoly over the legitimate use of force, rightly so given the destabilization that would ensue in relations between nation-states. More recently, the private sector itself has been asking for the rules to be clarified. It is important for states to respond to this demand, but by closely involving firms in discussions about how to regulate cyberspace.

[3] SMITH B. & BROWNE C.A. (2019) *Tools and Weapons: The Promise and the Peril of the Digital Age* (New York: Penguin Press).

The security of digital products and services is crucial to stability in cyberspace.

THE SITUATION: Many attacks take place because computer products (some of them widely used) and security systems are not updated. This lapse might be due to the absence of patches for well-known flaws, or it might occur because patches, though available, are not widely enough applied. Furthermore, software editors and equipment manufacturers do not systematically offer assistance for handling an attack and restoring their products return to a normal state of operation afterwards. Worse yet, distributors and integrators sometimes carry software versions that are obsolete or cannot be updated, or they even distribute products known to lack security. Such comportment is unacceptable. It transfers to users the risks related to their systems and data, and might even — if such products are in mass use — have a systemic impact that jeopardizes the stability of the whole information system or of cyberspace itself.

All parties in the supply chain (from design to integration, deployment, maintenance and the management at the end of the product's life cycle) have responsibilities in this situation.

SOLUTIONS: To reinforce international stability and security in cyberspace, a consensus has gradually taken shape among governments about the importance of establishing at the international level a principle of responsibility for private entities. In 2017, this proposal was agreed upon during the negotiations conducted within the UN group of governmental experts (GGE) on cyberspace. Although the GGE's report was not adopted because states did not agree on another point (namely, the conditions for applying international law in cyberspace), French diplomats have followed up on this work. Jean-Yves Le Drian, minister of European and Foreign Affairs, presided over a meeting on this topic that was held on the sidelines of the UN's General Assembly in September 2017. This initiative led, the following year, to the "Paris Call for Trust and Security in Cyberspace" and to further technical discussions at the OECD.

At stake is to set minimal security requirements for products and for the systems incorporating them. The use of certificates of security is to be encouraged or even made compulsory for critical components in sensitive sectors. Such a measure will not suffice however.

What is needed is a much deeper reinforcement of a "culture of security". Firms should be encouraged to take proactive measures to continuously maintain the security of their products: monitoring, reviews, the training of product development teams, the organization of "bug bounties", transparency about detected flaws, etc. Patches must be made accessible as widely as possible (even in the absence of a maintenance contract) within a reasonable time once a vulnerability has been reported to the manufacturer.

Offensive actions by nongovernmental actors in cyberspace should be prohibited.

THE SITUATION: Given the multiplication and sophistication of cyberattacks against private entities, and regardless of the motivations (economic espionage, ransoms, attempts to tarnish the reputation, etc.), firms have been urged to adopt passive defenses: firewalls, antivirus programs, rules of cyberhygiene, etc. As we are forced to admit however, such measures are not always well applied and do not offer full protection. For one thing, they only protect against threats that have already been identified. For another, the prospects of recovering assets after an attack are far from certain. Although filing a complaint is highly recommended, the victim can never be sure that judicial procedures will lead to identifying the parties behind an attack and obtaining compensation.

Some entities might prefer an active to a passive defense. Measures of active defense (tracking data, neutralizing the infected machines used for botnets, disseminating markers with information about third-party servers) might affect a third party's information system. Pushed to the limits, such measures could involve "hacking back" with the use of highly intrusive means (blocking devices, recuperating data, sabotaging…). This would amount to the use of force in cyberspace. To hack back, the victim of an attack might rely on his own resources and capacities or else on subcontractors ("mercenaries") who are equipped to conduct an offensive action.

Let us be frank: it is not acceptable for non-state actors (NSAs) to carry out offensives of this sort. Not only does this negate the state's monopoly over the use of force, it is contrary to international law. Furthermore, it very much risks destabilizing cyberspace. Imagine a private party who has decided to use any and all means to recover his stolen data. After attributing the responsibility for the attack, he tries to neutralize the infrastructure used by the presumed hacker. But this action might unexpectedly lead to destabilization and escalation. Blaming an attack on a specific party is a decision with a margin of error that nation-states alone should assume. Furthermore, acts of retaliation might cause serious collateral damage. When (as often happens) they are conducted on the territory of another state, the latter might consider that its sovereignty has been violated and respond.

SOLUTIONS: According to the French national strategy of cyberdefense, what should be done is to "*advocate the prevention of cyberoffensive capacities being used by NSAs and support the prohibition against NSAs conducting offensives in cyberspace for themselves or for the benefit of other NSAs, except in very precise cases and on condition that the technical actions imagined are tightly overseen. […] Such rules are to be precisely defined on the technical level so as to draw a clear, controllable line acceptable to all.*"[4] What qualifies as an offensive action (which should be outlawed for private actors under all circumstances)? And what qualifies as a legitimate act of active defense (which could be authorized under the condition of oversight)? Answering these complicated questions will take time. Discussions have been organized at the request of France within the OECD's Global Forum on Digital Security for Prosperity. It is important to involve the private sector.

[4] SGDSN [SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE] (2018) *Stratégie nationale de la cyberdéfense* (Paris: Economica).

The marketing of devices, software or techniques that are likely to be misused should be controlled.

THE SITUATION: In recent years, private firms have developed and marketed intrusive, destructive software. Such software is a cyberweapon. It is difficult to thwart the proliferation of this weaponry. Owing to the characteristics of this market and the products on it, determining whether such software has a defensive or offensive finality is no easy task. The risks arising out of the proliferation of these weapons have been agreed upon at the international level. In 2015, the GGE reached the conclusion that states should prevent the proliferation of malicious software and devices. The process of regulation started when "intrusion software" using encryption was added to the Wassenaar list of "*dual-use goods, technologies and munitions*" in 2013.

SOLUTIONS: The task of defining "intrusion software" should be pursued. Thereafter, the question will arise about a tighter system for authorizing the marketing of tools that, like weapons of war, have a destructive potential.

Conclusion

The security and stability of cyberspace cannot be the responsibility of nation-states alone. Input from the private sector is needed. Although this sector is not the appropriate party to set the rules, it does have a key role to play in promoting good practices that should eventually become standards and in taking part in discussions prior to the adoption of new, legally binding regulations.

The form that these rules will take is yet to be determined. Depending on the responsibility assigned to firms, these rules might take the form of obligations or recommendations. They will have to be formulated so as to make the imperative of security compatible with the protection of innovation. The role and size of the entities concerned will also have to be taken into account: those that have a systemic role should assume more responsibility.