INFO FLASH
Finabel
European Army Interoperability Centre

The challenge of digital sovereignty

WRITTEN BYANNABELLE BOURDAS

https://unsplash.com/photos/iar-afB0QQw

INFO FLASH
Finabel
European Army Interoperability Centre
The challenge of digital sovereignty
By Annabelle Bourdas

With the recognition of cyberspace as a domain of operation, conducting covert cyber espionage and cyber interference has become more accessible, threatening public institutions and global companies. Hence, cyberspace plays a part in modern warfare. It offers many opportunities but also brings great challenges for national security.

A striking example of this modern/ hybrid warfare was the cyber-attacks in Estonia in 2007. This event marked how foreign interference can damage a whole country; it also showed cyber-attacks' efficiency when exploiting vulnerabilities within virtual systems. Indeed, online services such as banks, public institutions and media channels were affected as the servers were overwhelmed with internet traffic, creating an overall feeling of confusion and eventually leading to chaos.

States have started to develop their cyber armies by forming cyber combatants. There was a shift from ensuring cyber defence to enhancing offensive or fighting capabilities in cyberspace. More governments are trying to master essential technologies to ensure their digital sovereignty. Indeed, it has now become cheaper, faster and easier to conduct cyber-attacks. As a result, the number of cyber-attacks has expanded over the years. Moreover, the range of actors and targets has grown. Nowadays, every industry can be targeted, from the agri-food industry or hospitals to public institutions.

In France, the Defence Intelligence and Security Directorate is in charge of protecting personnel, information, material and sensitive installations of the national defence. It aims at protecting companies that have a national interest from cyber-attacks. To adapt to this technological revolution, companies have gone through a digital transformation as big data, cloud, or artificial intelligence have caused companies to rethink their business model and production capabilities. Hence, there is now a focus on how to protect the companies' or public institutions' infrastructures from external intrusion and cyber-attacks (Bucquet, 2021).

Regulation of these cyber-attacks is complicated as new technologies evolve rapidly and legislators cannot keep up with them. There is also the attribution problem, meaning that these attacks can be conducted by anonymous hackers or by state-sponsored hackers, and tracing attacks' origin to attribute it to someone can be difficult. State-sponsored hackers also have to maintain discretion as the state behind the attacks has to be able to preserve the possibility of denial. This is problematic because perpetrators cannot be prosecuted if they cannot be found.

Furthermore, the European Union (EU) is also trying to regulate these cyber operations within the Common Foreign and Security Policy (CFSP). Since June 2017, the EU has developed a cyber diplomatic toolbox. This would allow the EU to have a joint diplomatic response, including sanctions. These measures would be "proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity" (Council of the EU). In 2020, the EU made use of this toolbox to impose restrictive measures that act as a deterrent on several individuals and entities involved in various cyber-attacks such as WannaCry, NotPetya, and Operation Cloud Hopper (French Embassy in the UK).

Moreover, the EU has expanded its mechanisms to build up digital sovereignty, such as the Directive on security of network and information systems (NIS Directive). The NIS Directive came into force in 2016 as part of the EU cybersecurity strategy, which is the first legislation on cybersecurity at the EU level. It aims at increasing the protection from cyberattacks in the EU. Since 2020, the Directive has been modified by expanding the scope of protection to new sectors. Moreover, the EU Cybersecurity Act, which entered force in 2019, has provided the EU with a framework to certify products, services and processes. The EU Cybersecurity Act has also strengthened the mandate of the EU Agency for Cybersecurity (ENISA) (European Commission).

The EU cybersecurity strategy tackles the geopolitical competition in cyberspace particularly, since the Covid-19 pandemic. The EU is working on building capabilities to prevent cyber-attacks and defend itself against them about the Cyber Defence Policy Framework (CDPF) which was adopted in 2014. The CDPF aims to develop the Member States' cyber defence capacities. Indeed, cyberspace is the fifth domain of operations after land, sea, air and space. Hence, the success of cyber operations relies on "uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber operational capabilities" (European Cyber Defence Policy).

Again, cyber-attacks can be conducted by state-sponsored hackers for purposes of destabilisation, sabotage or computer espionage. "Foreign interference tends to be regarded as conduct by foreign actors or their proxies that is covert, deceptive, and against the target state's national interests" (Dowling, 2021). Cyberspace has no physical boundaries, which blurred the lines between domestic and foreign barriers as foreign interference now forms of cyber interference. This new type of foreign interference raises new challenges and questions such as whether these attacks could be an act of war? How we categorise these attacks and how we regulate them will have an impact on the conduct of cyber operations.

In conclusion, the number of cyber-attacks has increased in recent years. Companies have felt the need to adapt to new technologies. However, this digital transformation has made new challenges appear. "Countering information interference remains problematic due to legal, ethical, detection and mitigation dilemmas" (Dowling, 2021).

As companies and public institutions now rely on their virtual infrastructures, they have been exposed to malicious actors who plan on exploiting their systems' vulnerabilities. The emergence of new profiles of hackers and the hybridisation of work, the fast-paced evolution of new technologies, their availability on the market and the sophistication of the operating modes have made governments and the EU develop tools to create digital sovereignty and help companies protect themselves and the national interests they serve from cyber-attacks (Bucquet, 2021).

Bibliography

Bucquet, E. (2021, November 24th) Cyber threat: the DRSD on the front line (“Menace cyber : la DRSD en première ligne)
Available at : https://www.revueconflits.com/menace-cyber-la-drsd-en-premiere-ligne/

Council of the EU. (2017, June 19th) Cyber attacks: EU ready to respond with a range of measures, including sanctions.
Available at:
https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

Dowling, M-E. (2021, March 31st) Democracy under siege: foreign interference in a digital era, Australian Journal of International Affairs.

European Commission. (2022, May 13th) Commission welcomes political agreement on new rules on cybersecurity of network and information systems.
Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_29805

European Cyber Defence Policy. (2014, November 18th) The European Cyber Defence Policy
Available at:
https://www.european-cyber-defence-policy.com/#:~:text=The%20EU%20Cyber%20Defence%20Policy%20Framework%20(CDPF)%20supports%20the%20development,legislation%2C%20including%2C%20when%20it%20is

French Ambassy in the UK. (2020, July 30th) EU imposes sanctions for cyber-attacks.
Available at: https://uk.ambafrance.org/L-UE-impose-des-sanctions-contre-des-cyberattaques

Picard, S. (2021, October 15th) Integrating cyber operations into modern warfare (“Intégrer les opérations cyber à la guerre modern »)
Available at: https://www.revueconflits.com/integrer-les-operations-cyber-a-la-guerre-moderne/