The Crucial Challenge of Cyberthreats

Jean-Louis Gergorin, former Director of the Ministry of Foreign Affairs' Policy Planning Staff (CAP), is co-author of *Cyber. La guerre permanente*, Paris, Cerf, 2018.

Thomas Gomart is Director of Ifri.

Marc Hecker is Ifri's Director of Publications.

Translated from French by Philolingua, edited by David Quin.

Jean-Louis Gergorin

We are currently witnessing a strategic revolution that I would call a merger between Sun Tzu and Clausewitz, two of the greatest strategic thinkers, with the first one being the most famous in the West. Clausewitz said that war is the continuation of politics by other means, since war is an expression of violence in order to achieve the objectives of control, influence, etc. Sun Tzu simply wrote, 2,500 years ago: "The supreme art of war is to subdue the enemy without fighting". This is consistent with what Professor Mahbubani said: the Chinese strategy is to win, to prevail by avoiding war. The Chinese have remained loyal to Sun Tzu.

Cyberwar is the fusion of two lines of thought, because it makes it possible to achieve the objectives of control and influence that Clausewitz described, in an attempt to continue politics through non-violent methods – in any event at the start, since, for example, if you cause an air disaster by blocking navigation systems, it becomes very violent. In any event, cyberwar for the most part can be non-violent, and achieve exactly the same control objectives as politics and war, and much more effectively.

What is cyberwar?

Another important thing is to know what we are talking about when we talk about "cyberwar" – and I know that this is not straightforward. Cyberwar is the offensive use of all digital options for control purposes, and this can be done in two major ways. The first is hacking for espionage, sabotage or intimidation purposes – and is currently the most common form.

"Cyberbullying"

We don't talk about "cyberbullying" a lot, but it's definitely important. I will give you three recent examples in chronological order. In May 2018,

German cybersecurity officials reported a series of hacks in the energy and electrical systems, attempts that were seemingly foiled. There was no official attribution – that is the policy of BSI, the German cybersecurity agency – but the head of the State Office of the Protection of the Constitution accused Russia, and that has not been denied or confirmed. Second example: the United States' Department of Homeland Security published a well-substantiated report in July 2018 where it revealed that more than four hundred US electrical facilities – distribution and generation – had been subject to penetration without sabotage. The Americans also emphasized that their enemies could have committed sabotage, that they did not, but had shown that they could do it and could return. I am convinced that those who did this – the Americans have clearly attributed the operation to Russian military intelligence, the GRU – wanted to show that, in this period of tension and sanctions, they could act at the center of the US system. The third case, which involves us directly: Guillaume Poupard, head of the National Cybersecurity Agency (ANSSI), said in January that significant pre-positioning – that is to say penetration without sabotage, like that described by the Americans, showing that the entity that did this is able to return and sabotage – had occurred in France and allied countries (Germany). This is strategically critical. We are very committed to our independence, to our deterrence, etc, and foreign entities have shown that they could paralyze us and, for example, deprive us of electricity for several hours.

Manipulation of information

The second approach of cyberwar, the manipulation of information, is very different from hacking. This manipulation of information can be done through manipulating social media, which is an extraordinary vector of information. The problem of fake news is very subjective. What is not subjective, on the other hand, is the problem, which must be measured objectively, of fake profiles on social media. If you say you're Louis Durand, a truck driver in Rouen and a Yellow Vest and you're running an extremely active and violent Facebook account, but you're actually John Stuart working for M. Shillman (a far-right US billionaire who is highly active on social media against the European Union), or if you are Mr Popov working at the Internet Research Agency in St Petersburg, and you pass for Louis Durand either way, you can do a lot of harm behind this fake profile.

I myself followed (having found it online), between the end of August and the end of December 2018, a person raging on Twitter under the name of A. Dupond III, who retweeted all the messages from the French

cyberspace that were most hostile to President Macron and his policies (caricatures, photos of people with fake injuries during the Yellow Vest protests, etc) – which amounted to 40,000 tweets during the period quoted. He started at six in the morning and finished at ten in the evening.

Digital manipulation

I will finish with two examples of digital manipulation of information in cyberwar. *Deepfakes* are digital manipulations of videos by artificial intelligence, that is to say "neural networks". Currently, it is almost impossible to detect a fake video, and it became technically possible to create a false conversation – for example yesterday – between Theresa May and Emmanuel Macron, by making it appear true; experts will be able to dissect it to see if it is true or not using other neural networks. In times of elections, you can therefore manipulate public opinion by releasing a false video. You can also – it is a new invention that appeared two or three months ago – rig GPS information, information of maps on Google Maps, create fake visual information or navigation, which can have a profoundly destabilizing effect.

Thomas Gomart

First, I will emphasize the term "threat" that appears in the title of our session: it reflects a fairly recent development in our understanding of cyberspace. Until the Snowden case, cyberspace was most often presented as a tool of liberalization and extreme individualization; since Snowden, a reversal has occurred, to the extent that this matter has made not the specialists but also the public aware of the power of what could be called "the military-digital complex". The "opportunities opened up by cyberspace" aspect is now overshadowed by the "threat" aspect, and this swing refers back to military logic and libertarian roots. This duality, in my opinion, dominates today.

Who is threatening whom?

Second comment: when we talk about threats, who formulates them and who experiences them? We need to distinguish the three types of actors we have to deal with when talking about cyberspace, as well as infrastructure that can be affected by these threats. The main types of actors are, first, states – and we are witnessing quite a remarkable "return of states" in terms of Internet governance; then there are the platforms – GAFA [Google, Apple, Amazon, Facebook] and BATX [Baidu, Alibaba, Tencent, Xiaomi] – and finally individuals, surfers and users. Essentially, there are three layers that are affected by different types of threats: the hardware

layer – infrastructure, submarine cables, *data centers,* for example – the application layer that brings the different applications together, and the cognitive layer.

We must keep these three actors and these three layers in mind to properly identify the type of threat we may face.

I will, not surprisingly, quote Raymond Aron, who points out the opposition – in my opinion at the heart of our difficulties in thinking about cyberspace – between what he calls the necessarily limited "economic behavior" for the decision-maker and what he designates the "diplomatic-strategic behavior" that is made "in the shadow of war". This tension between economic behavior and diplomatic-strategic behavior must also be at the heart of our thinking about cyberspace. Essentially, the important point is the simultaneousness of these two behaviors and the capacity that we have or not to monitor them concomitantly.

Digital power and types of threats

I will finish off my remarks with a few quick points. The first concerns the concept of digital power to try to identify the main threats. I will use the image of the chessboard and the web – and you must think about both simultaneously. On the chessboard, the pieces have a value relative to each other and are part of a hierarchy – and this is a key, for example, to interpreting inter-state relationships of a conventional nature. On the web, everything basically depends on the number of contact points you can have, and it can be unlimited.

The second aspect of digital power: the importance given to network power. Network power is this paradox that we all experience using our search engines: the use of standards by a growing number of users strengthens this standard, but, in doing so, reduces the possible options and choices. Whoever exercises network power gains decisive influence in this logic.

The third comment about digital power: digital technology forces us into a debate between sovereignty relationships (those used to make collective decisions) and social relationships (those used to make individual decisions). The burgeoning literature on cyberspace raises the question: who will prevail and what type of relationships will have primacy?

This leads me to try to identify the main threats. I will begin, taking the previously defined actors as a starting point, with the state-to-state

relationship in digital technology. The main problem here is attribution. We cannot have attribution mechanisms in cyberspace comparable to those of a conventional or nuclear battleground: by explicitly attributing an attack, you show your own capacity in your understanding and knowledge of the other. A second type of threat can be observed in the relationship between states and platforms. We are in a problematic situation – for Europeans – that is implicit in previous round-table discussions. Some platforms now have investment capacities vastly superior to that of states, and have very powerful marketing power. The Paris Call for Trust and Security in Cyberspace is proof of this, a way for some of the platforms to redeem a form of virtue for themselves after demonstration of their collusion with some states, particularly the United States.

The third type of threat is observed in the relationships between platforms and individuals. The Europeans' response is the famous GDPR (General Data Protection Regulation) that is supposed to protect each consumer's data with respect to the large platforms. However, not everything is protected, particularly in the area of security data.

Finally, a fourth type of threat can be observed in the relationship between states and individuals. This is where the differences in political regimes affect most directly: setting up forms of digital authoritarianism with facial recognition, or the social credit that the Chinese authorities are developing and that will have consequences in what are called *smart cities*. The actual security aspect is becoming a component of the smart city, and hence of how to govern.

All these issues are decisive for Europe, which at present is adopting an ethical position. Clearly, this is important, with the debate on the future of artificial intelligence, but it is not sufficient. The fundamental issue for the Americans, in terms of cyberthreat, is their industrial and military capability to react. And the second striking aspect – and this is also a serious "threat" – that we are now witnessing, in every speech promoting individualization, is digital technology refocused in the hands of a few actors.

Marc Hecker

My question concerns the three layers you have just defined. Is there a hierarchy of threats within these layers? And are these layers vulnerable in the same way? I am thinking particularly about the physical layer, which should allow us to talk about common areas. You mentioned in your last book that 95% of telecommunications and digital data are transmitted by submarine cables and that there are only 448 cables coming to

around 100 landfall points. Are these cables vulnerable, and is this material vulnerability underestimated compared to other threats highlighted for the cognitive or software layer?

What are the specific vulnerabilities?

Thomas Gomart

This vulnerability was indicated in studies in the *Revue stratégique* and *Revue de cyberdéfense*. These cables can be severed, as we have already seen; they can be spied on by submarines, and this has also happened recently. One industrial development is important to note: some platforms are now acquiring their own resources to become cable installers, to lay their own cables, in a form of vertical integration, without saying so openly. This raises the question of a possible analogy with the energy sector: the Europeans must clearly separate what comes under the infrastructure layers from what comes under the application or cognitive layers. The vulnerability of these cables is therefore real, like the much more dispersed one of data centers.

Jean-Louis Gergorin

I would like to issue a warning. One of the main characteristics of cyberthreats is that they keep on increasing and that they will increase in the form of hacking. We will witness a tripling in the number of connected objects, and we will have more than 20 billion in two or three years, which will significantly increase the risks. Furthermore, the Internet of Things requires a vector to transmit information, which will be 5G; that is to say, a considerable acceleration capability through cellular networks. And from that perspective, vulnerability will also increase.

We must not fall into a paranoia that would proscribe Huawei – there are lots of things that Huawei does that don't cause a problem. Nevertheless, there are security nodes that any sovereign state must absolutely maintain, and the Europeans must be able to control these nodes. Yet, the resources assigned to this problem (there will be a so-called "Huawei law" in France and provisions have already been made in Britain and Germany) are too limited to even deal with the sole problem of 5G. Not to mention other cyberthreats.

We need to be aware of the gap that exists in cyber capacities between the different states. In France, the bodies that are responsible for cyberspace – in broad terms, ANSSI, DGSE (Directorate-General for External Security), Cyber Defense Command – account for 3,500 people. In Germany, there are just over 2,000. In the UK, everything is concentrated,

whereas it is somewhat fragmented in France and Germany. In the United States, there are 50,000 in the NSA. In Israel – already a great power in the making – there are 6,000 people in UNIT 8200. If you now consider the annual technological investments in cyber start-ups, they represent 30 million in France – dollars or euros – 42 million in Germany, 300 in the United Kingdom, 3 billion in the United States and 600 million in Israel. Therefore, there is still a significant effort to be made, and it must begin with a Franco-German rapprochement, since the British are bound by agreements with the Americans.

As for social media, we have seen their major importance in politics. It is obvious that we cannot accept a completely asymmetrical situation where authoritarian countries would control the Internet and use it for social control. Russia is starting to be inspired by China, which controls the entire Internet. There is British draft legislation to make the heads of social media accountable; but here too we also need a European response in the face of social media, or at least a Franco-German one. Therefore, I want to issue a double call for action. The dangers are both deep and real.

Europe in the face of cyberthreats

Marc Hecker

I would like, to conclude, to pick up on your comments, and ask you both what your recommendations for Europe are on the issues related to cyberspace.

Thomas Gomart

There is an urgent need to distinguish the data covered by GDPR from that which is not. Jean-Louis Gergorin encouraged Franco-German reflection on the issue, and I share his point of view. An Ifri study published in July also shows how much debate there is between experts to determine whether we should promote the Franco-German partnership or whether these issues should be integrated in the more traditional P3 framework. The debate is not settled, and, in my opinion, it deserves to be expanded to all European countries. There is an urgent need to better define the data without believing that GDPR protects us from everything.

Jean-Louis Gergorin

My recommendation involves industrial and technological policy. Last week, I had the privilege of being invited to a meeting organized by the European Union where there were some very high-level Britons, including the head and technical director of the British Cybersecurity Agency,

which has produced the only comprehensive report on Huawei and 5G. What I can remember is that we have created our own problems ourselves. No-one reacted to Huawei's dumping. There is a Commissioner for Competition in Brussels, there is a competition policy, but no-one was concerned about the fact that one actor enjoyed a dominant position, while Alcatel for example has been eliminated, Nokia has been weakened, and Siemens has got out of the business. This is an industrial issue where the European Union has been inadequate.

Furthermore, it should be pointed out that Europe is spending a lot. Since 1960, it has spent 80 billion in current euros on the innovation policy, whereas the US DARPA [Defense Advanced Research Projects Agency] spent only 60 to 65 billion euros over the same period, but is the source of a lot of things in the area of artificial intelligence (Internet, microprocessors, etc). We must spend our money better, and debureaucratize. An initiative was launched by a Franco-German partnership to debureaucratize innovation, to have agile organizations, to emerge from the paralyzed mechanisms that we currently have. Manufacturers are delighted to have additional subsidies, but this won't allow us to reinvent the future. We must change the method and adopt more flexible methods – that is the meaning of this initiative that I wanted to welcome.

PF