CSS Analysis in Security Policy

CSS ETH Zurich

No. 71 • April 2010

CYBERWAR: CONCEPT, STATUS QUO, AND LIMITATIONS

Political, economic, and military conflicts are increasingly also being carried out in cyberspace. However, conceptually, the notion of "cyberwar" only includes a narrow sub-section of all conflicts in cyberspace. At the operative level, capabilities for cyberwarfare are becoming increasingly important. Nevertheless, the prospects for strategic IT wars that only take place in the virtual space remain extremely unlikely. For many states, there is a particular need for action in the area of cyberdefence.

Istock.com

The importance of the information space as a theatre of conflict has increased in recent years. Every political, economic, and military conflict today is carried out to some extent on the internet. In this context, the term "cyberwar" is a frequently-used buzzword. It often refers to any kind of conflict in cyberspace with an international dimension. However, such a broad use of the term is not very useful. What is required instead is a conceptual categorisation of various forms of conflict in cyberspace. This is an indispensable precondition for assessing the concrete danger and its importance, allocating responsibilities, implementing preventive and reactive countermeasures, and conducting criminal investigations.

The term "cyberwar" only covers a narrow sub-section of all cyberattacks. From a military point of view, it should be regarded as part of information warfare. In order to determine the substance and relevance of the concept of "cyberwar", we require not only a lexical definition, but also a differentiation between the operative and strategic dimensions of cyberwar. We must also distinguish between offensive and defensive cyberwar measures, with the role of the military in cyberdefence being a limited one.

Cyberwar as a sub-concept

In practice, it is becoming increasingly difficult to categorise cyberattacks primarily according to the perpetrators involved. Since the ability of attackers to conceal themselves is constantly improving, it is often impossible to identify them clearly and promptly. Nevertheless, the intention of an attack, as far as it can be established, is of conceptual importance, as by no means all cyberattacks have a military origin or are part of a cyberwar. Another important distinguishing feature is the potential damage caused by an incident. This notion is connected to the image of a cyberladder: The further up the ladder the nature of the attack is, the greater its potential damage.

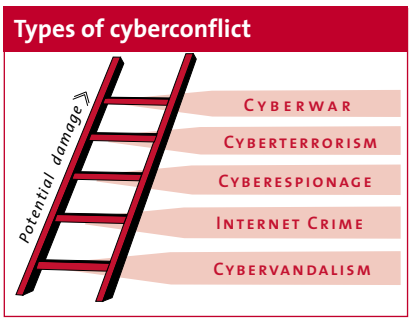
On the first rung of this ladder are cyber-hacktivism, or cybervandalism. This involves virtual modification or destruction of content, e.g., hacking websites or disabling a server by data overload. Cybervandalism is the most widespread form of cyberconflict and garners a great deal of public attention. However, the effects of such incidents are limited in time and relatively harmless.

On the second and third rungs are internet crime and cyberespionage. Both are routine occurrences that take place independently of conflicts. The main victim in these cases is the corporate sector: Even though it is very difficult to secure reliable data, the global costs of these phenomena are estimated to lie in the range of US$1 trillion annually. Government networks with classified data are also affected, but are targeted comparatively rarely.

On the fourth rung, the term "cyberterrorism" is used to describe illegal attacks by non-state actors against computers, networks, and the information stored therein, carried out with the aim of intimidating a government (or population) or to compel certain behaviour. A cyberattack is therefore only categorised as cyberterrorism if

it results in physical violence against persons or property, or at least causes sufficient damage to create considerable fear. The potential scope of damage is regarded as very high, although there have been no real-life cases of cyberterrorism to date.

The top rung of the cyberladder is cyberwar. The term refers to warlike conflict in the virtual space that primarily involves information technology means. The term "cyberwar" refers to a subsection of information warfare. As part of this broader concept, which aims at influencing the will and decisionmaking capabilities of the enemy's political leadership and armed forces and/or the attitudes of the civilian population in the theatre of operations at the level of information and information systems (cf. CSS Analysis no. 34), cyberwar includes activities in cyberspace. Conceptually, therefore, cyberwar reflects the increasingly technologised nature of war in the information age based on computerisation, electronisation, and the networking of nearly all areas and aspects of the military.



Within the concept of cyberwar, a distinction must be made between three forms of Computer Network Operations (CNO): The deliberate paralysation or destruction of enemy network capabilities is called a Computer Network Attack (CNA). Such attacks may be complemented by Computer Network Exploitation (CNE), which aims at retrieving intelligence-grade information from enemy computers by means of IT. Finally, Computer Network Defence (CND) includes measures to protect own computers and computer systems against hostile CNA and CNE.

Operative reality

The potential for damage that a cyberwar can inflict on the security and welfare of a state is enormous. However, CNA capabilities today should be regarded mainly as one of many operative instruments in the framework of military missions. The importance of this instrument will certainly increase globally in the coming years. However, scenarios for a strategic cyberwar, i.e., a conflict conducted exclusively in the virtual realm, remain unrealistic at this point.

With regard to the state of developments in offensive cyberwar capabilities, there is a lack of established knowledge at this time. Therefore, unlike in the discussion over the lower rungs of the cyberladder, the debate on cyberwar is extremely prone to speculation. There is no doubt that CNE is already a reality today that cannot be reversed. Thus, the insecurity is mainly related to the extent of CNA capabilities that are already available. Some of the estimates in this area seem exaggerated or unfounded.

Examples of potential CNA applications are frequently advanced. For instance, the US is alleged to have switched off local mobile telephone and computer networks during its occupation of Iraq in order to prevent insurgents from coordinating their attacks. In the aftermath of an Israeli air strike on a supposed Syrian nuclear installation in September 2007, too, speculation was rife as to whether Israeli aircraft might have been able to enter Syrian airspace due to a cyberattack on the Syrian air defence system. However, such reports must always be carefully scrutinised, especially since they often treat cyberwar as being synonymous with information warfare, and as it remains unclear whether CNA capabilities were really deployed.

The indicators used by intelligence services to identify CNA capabilities such as doctrine, training, simulation, or industrial cooperation have only limited significance. However, it is undisputed that offensive cyberwar capabilities are a major issue in the US. At the Pentagon, an infowar team has been tasked with building such capabilities since 1999. In 2002, then-US president George W. Bush ordered the elaboration of a strategy that would define guidelines and criteria for conducting cyberwar. It is unclear to what extent such efforts have come to fruition, however. France, Israel, Russia, and China are also rumoured to have offensive capabilities. The German armed forces, according to media reports, are in the process of establishing a unit for "Information and Computer Network Operations" that is alleged to have CNA capabilities. Other states are discussing the development of such capabilities. However, the debate is in many cases still in its infancy.

Strategic cyberwar?

Cyberwar is frequently presented as a new kind of war that is cheaper, "cleaner" (with less or no bloodshed), and less risky for an attacker than other forms of armed conflict. Such positive assessments are frequently linked to the expectation that the future will bring not only an arms race in cyberspace, but also strategic cyberwars. However, it seems appropriate to question some of these assertions.

Thus, considerable doubt remains as to whether strategic cyberwar is really feasible. According to experts, it is still not possible today to conduct targeted cyber-based attacks. This view, conversely, places a question mark over the logic of strategic cyberwar as such. Uncontrollable blowback effects in the highly networked virtual space constitute considerable risks for the attacking state as well. This factor is all the more important since the states that are most likely to have or to develop the technological know-how for strategic cyberwar are also most dependent on their own information infrastructures and thus highly vulnerable in an IT war. Due to uncontrollable side-effects, a cyberwar would also undermine trust in cyberspace over the long term, with possible detrimental effects for the global economy and thus for all parties involved. Furthermore, the development of such cyberwar capabilities is probably much more costly than is generally acknowledged.

From a legal perspective, too, the offensive dimension of cyberwar is controversial; this applies to cyberwar both in its strategic and in its operative manifestations. The reason is that in cyberwar, civilian and military targets can no longer be distinguished, and civilian infrastructures are intentionally targeted. It is unclear whether, under international law, the use of computers in cyberwar can be considered "use of weapons" and "use of military force". It also remains to be clarified to which extent mere intrusions into computer networks as part of CNE by a state entity for the purpose of information-gathering can be considered violations of international law.

Defence: Limited role of the military

Against the background of the considerable imponderables as far as offensive cyberwar capabilities are concerned, there

have already been calls for cyber-arms control. However, at this point, it is unclear how a mechanism in this area could be implemented effectively, for instance in the area of verification. An alternative process could be based on political statements of renunciation of such capabilities, but many states will most likely be loth to restrict their options too far in this regard.

In either case, it must be assumed that the majority of the armed forces will be engaged more in cyberdefence than in offensive capabilities in the coming years. Computer Network Defence is already a very important issue today. Attacks on information technology, manipulation of information, or successful espionage can have massive detrimental effects on the effectiveness of one's own armed forces. Accordingly, military networks must be secured against all forms of cyberconflict.

However, CND as a concept is limited to military networks. Countermeasures at all levels of the cyberladder, whether preventive or reactive, are dominated by civilian measures. The emphasis on the importance of civilian actors in this area is useful, not least because in terms of the number of real incidents and the estimated damage created, internet crime (combined with cyberespionage) is by far the most grievous problem that the international community of states is confronted with today.

Countermeasures at levels one through three include information assurance, which is the responsibility of each individual citizen and company, as well as measures under private and criminal law. The state should protect its own networks and, through its legislative bodies, ensure that any existing gaps in internet law be closed. In this context, international cooperation is also of great importance. At level four, if not before, these aspects are complemented by critical infrastructure protection (cf. CSS Analysis no. 16). Such protection concepts primarily require close civilian partnership between the state and the corporate sector as well as intense inter-state cooperation. However, the military may provide important contributions in identifying enemy disinformation or protecting national command-and-control structures.

Cyberwar in Switzerland

In Switzerland, the building of capabilities for conducting information operations has hit an impasse in recent years (cf. CSS Analyses no. 34). This is due among other factors to legal ambiguities, financial and personnel shortfalls, and political reservations, for instance with regard to psychological operations. As far as the sub-sector of cyberwar is concerned, some initial steps have been undertaken at the level of the armed forces. According to their own account, however, the Swiss armed forces are not yet able to detect a professional hacker attack on their own infrastructures and to react to such an attack in an adequate and timely manner. The massive attack on the Foreign Ministry in October 2009 revealed the vulnerability of Swiss governmental agencies to cyberattacks.

At the Centre for Electronic Operations (CEO) of the Armed Forces Command Support Organisation, two cyberwar-related units are in the process of being established. The first of these is a military Computer Emergency Response Team (milCERT) whose task is to monitor the systems and networks of the armed forces and to sound the alert when required. One of the core challenges for this team, in addition to the personnel buildup, is coordination with the existing Government Computer Emergency Response Team (GovCERT), which is an important component of the Reporting and Analysis Centre for Information Assurance (MELANI).

On the other hand, the CEO is also in the process of building up a cell for Computer Network Operations. As far as its activities are concerned, the Federal Department of Justice and Police and the Foreign Ministry's Directorate of Public International Law released a legal opinion in March 2009 to the effect that the country's current legal basis for CND is sufficient, but that offensive CNA and intelligence CNE are currently only permissible under a state of defence (*Aktivdienst*).

According to its own statement (cf. legal opinion), the Federal Department of Defence intends to establish both CND and CNE/CNA capabilities. However, the focus of Swiss cyberwar activities today ought to be on defensive measures. Here, additional personnel resources seem to be required. The same applies to MELANI, by the way, which like the CEO is underfunded in international comparison. Another important requirement is close military-civilian cooperation in cyberdefence, which also includes the Cybercrime Coordination Unit Switzerland (KOBIK). Finally, effective cyberdefence also requires international cooperation; in this area, the Cooperative Cyber Defence Centre of Excellence in Estonia appears likely to develop into an important multilateral framework.

It seems advisable to consider the establishment of CNE capabilities for federal intelligence-gathering bodies for activities outside of wartime situations, which would also be in line with the international trend. However, the creation of appropriate legal foundations is likely to be politically controversial. For instance, it would be necessary to ensure that CNE could not be misused for purposes of industrial espionage.

Where CNA is concerned, legal issues do not arise, as Switzerland would only use this capability in wartime if its own systems came under attack. The core question here is rather whether such a capability is feasible and necessary. Since this is a question of strategic importance, the appropriate authorities both in the military and at the political level should give due consideration to the matter.

Switzerland and cyberwar

- Legal opinion Swiss CNO (10 March 2009)
- Interpellation Schlüer on internet security (17 March 2009)
- Interpellation Segmüller on information operations (9 March 2009)
- Interpellation Graber on electronic warfare (18 December 2008)
- Foreign Ministry targeted by virus attack
- Armed Forces Command Support Organisation
- Reporting and Analysis Centre for Information Assurance (MELANI)
- Cybercrime Coordination Unit Switzerland (KOBIK)
- Cooperative Cyber Defence Centre of Excellence

- Author: Myriam Dunn Cavelty dunn@sipo.gess.ethz.ch
- Responsible editor: Daniel Möckli sta@sipo.gess.ethz.ch
- Translated from German: Christopher Findlay
- Other CSS Analyses / Mailinglist: www.sta.ethz.ch
- German and French versions: www.ssn.ethz.ch