OFFPRINT FROM STRATEGIC OUTLOOK 7

The Internet as a Military Arena:
a Challenge for the New Total Defence

Mikael Wedlin and Erik Westring

There is a fast growing dependence on the Internet for critical societal functions. New services are constantly being developed to replace existing ways of communicating. This has increased the significance of the Internet from a defence-related perspective. Intelligence gathering and influence operations, as well as covert military operations, are areas in which even in peacetime, the Internet has been used as new military tool. The digital battlefield will therefore be of major importance in the development of modern total defence. It is vital that Sweden stays abreast of the latest technical, organisational and legal advances.

That the Internet can also function as an arena for military activity is not a new idea. When FOI began to study IT warfare in the second half of the 1990s, research proceeded on the assumption that this would be the future of warfare, and that mines and missiles were history. Especially worrying was the expectation that our critical infrastructure could be digitally influenced or seriously disrupted. Now that Internet operations have become a reality in ongoing conflicts, it is possible to determine what a realistic future might look like. We were correct in guessing that the Internet would become a major part of daily life; no part of life today is untouched by Internet-connected systems. The influence of the Internet arena on current conflicts, however, has not created digital attacks that knock out entire societies, as was feared. Instead, it is in the phase immediately prior to an armed conflict that the Internet has been used most.

Even if we are now beginning to understand the mechanisms of warfare on the Internet, it is still extremely difficult to predict the future of the Internet as a whole with any precision. The first Swedish Internet bank began in 1996, but it is only in the past five to ten years that the Internet has become the *de facto* foremost communications channel for banking transactions. Almost all the services that we take for granted today, such as Google, Facebook and YouTube, were created in the past 20 years. It is possible to predict with a reasonable degree of certainty, however, that the Internet will continue to be significant for all sectors of society, and that its significance will probably increase. One could even go so far as to claim that the Internet will eventually lead to greater changes in lifestyles than those brought about by the Industrial Revolution in the nineteenth century.

The military challenges

Four of the Internet's characteristics create major defence and security policy challenges and specific military problems:

Anonymity on the Internet makes it relatively simple to conduct easily deniable operations. On the Internet, it is difficult to be certain that someone is really the person they claim to be. The legal legitimacy of a military intervention applies only if one can associate a military state actor with an activity, something that can be fundamentally difficult on the Internet. From a military perspective, this is an advantage if the aim is to act covertly and a disadvantage if seeking to defend oneself.

Thanks to the Internet, military operations can be conducted from a great distance. The Internet is a domain completely without national borders and "movement" can in principle be immediate and without distance. This means that operations on the Internet can be carried out from anywhere and, in principle, without any risk to military personnel. The absence of borders also gives rise to judicial ambiguity with regard to international law. Is placing malicious code on a mail server in a third country using someone else's territory?

The civil and military digital arenas share the same infrastructure. Military and civil threats have previously been separate. Sweden, in particular, has traditionally taken great pains to create a clear separation. On the Internet, however, military and civil threats flow into each other. This is particularly the case since it can be difficult to determine the origin, purpose and goal of an attack. If all the country's banks are suddenly taken down simultaneously, the antagonist

may be another state conducting an act of war or a group of bored or politically motivated teenagers. Such events are generally difficult to evaluate or analyse quickly. It is also difficult to determine which laws, if any, apply to IT attacks. Most of the conflicts in the Middle East have been accompanied by intrusions into web servers. Is this part of a military operation? Who is accountable? Does it make any difference if the sender is military? Sweden's greatest challenge is to achieve a division of labour between the armed forces and civil defence.

The Internet opens up cost-effective opportunities for asymmetric warfare. Attacks on the Internet are often of an asymmetric nature. Even small, financially strapped organisations or individuals can carry out acts on the web. The ability to conduct Internet attacks is entirely knowledge-based and a single individual with the right competences can disrupt even relatively large systems. Nonetheless, even on the Internet, generating large-scale disruption or long-term damage requires more substantial resources in the form of both intelligence capacity and time.

A clear example of this is *Stuxnet,* the attack on Iran's nuclear programme which was carried out by a computer virus targeted at the uranium enrichment facility in Natanz. A virus planted in the control systems destroyed a number of centrifuges and left the facility unable to enrich uranium. At the time of its discovery, this malicious code was among the most advanced ever seen. It was assembled from various different types of code written by several different programmers. With enough knowledge and time, however, it could have been written by a single person. To create successful code of this targeted type requires intimate knowledge of Iran's nuclear programme, detailed blueprints and access to both the hardware and the software one wants to attack – in this case, centrifuges – as well as the frequency converters that control them. The latter is essential to be able to develop malicious code that will destroy the centrifuges without triggering their in-built defences. Access to resources such as these is today only available to states.

Even if the Internet makes asymmetrical warfare possible, it is unlikely that someone with limited resources could achieve more than minor disruption. A strike against an entire sector of society would require a highly qualified adversary.

Fields of application of the Internet as military means

Traditional military means will still usually generate greater and more predictable effects than a cyberattack. For instance, the cyberattack on Ukraine's electricity supply during Christmas of 2015 was planned at least six months in advance and created a brief disruption, but the first subscribers had their electricity supply restored after a three-hour interruption. Traditional aggression against Ukraine's electricity supply would probably have caused more permanent, as well as more predictable, damage. The use of cyberattacks to cripple infrastructure is therefore likely be a complement to traditional capabilities. There are three areas in particular where the Internet is a particularly relevant arena for military operations:

For intelligence gathering. The Internet must be every intelligence organisation's dream. Information is located in a single location that is relatively accessible, and available in a format that can be gathered and processed automatically. It is evident that this is already happening on a massive scale, and that substantial resources are being allocated to information collection. An obvious example of this is the Snowden case, and the disclosures that resulted. There are also numerous published examples of illegal monitoring of organisations and individuals by the Chinese state.

As a platform and means for Influence Operations. The Internet has changed media habits and news-gathering methods in a fundamental way. Today, anybody can be a producer of information. Even in the well-organised information environment of the recent past, with only a limited number of information providers, it was difficult to identify a source. In today's media environment it is nearly impossible. False information that seeks to influence opinion can be spread with the efficiency of an epidemic. The flow of information is becoming an avalanche and actors in our neighbourhood are rearming in a goal-driven way on the Internet to use new digital media for their own geopolitical purposes. The 2016 presidential election in the USA is a worrying example. It is highly probable that future European elections will be exposed to the same kind of influence. The disruption of Ukraine's electricity supply in 2015 can also be considered an influence operation, which was probably done to instil

feelings of insecurity in the population rather than further any traditional military goal. The Internet has therefore ushered in new, more effective methods and tools for influence operations, and there is every reason to assume that their scale will continue to grow.

Covert operations in the grey and twilight zones. Deniability in Internet operations can be used in situations where a military operation is required but it is important that it is not understood as an act of war. The above-mentioned example of *Stuxnet* is typical of this category. It was an extremely advanced operation, but it is safe to assume that the sender did not want the hostilities to escalate into open conflict. Actions on the Internet also have a special significance in preparations for war and so-called pre-combat. In conclusion, it seems likely that the military uses of the Internet will affect populations most in peacetime.

International outlook

Several states have recently openly declared that they are in possession of a military Internet capability. This strengthens the assumption that the Internet will become a natural part of future military conflicts. Several times in recent years, for example, Russia has been accused of using data intrusion as a method of conflict. The *Stuxnet* operation was probably conducted by the USA and Israel, although neither has admitted this. China and Iran, among others, have also appeared in intrusion reports where it is reasonable to assume that a state actor lies behind the intrusion.

States have recently been shown to be very interested in information about other countries' infrastructure. Reports by US governmental organisations cite evidence that the USA's infrastructure has been mapped by foreign states. Sweden's National Defence Radio Establishment (FRA) reports that more than 10,000 "cyberactivities" are being directed against the country every month. According to the FRA, although the overwhelming majority of these are purely spying or other efforts to access information, at least one attempt to map Sweden's infrastructure has been identified.

After Estonia was heavily exposed to IT attacks in the spring of 2007, it established the Estonian Cyber Defence League, something resembling a "digital home guard". The aim is to strengthen society's capacity to deal with cyberattacks and to set up public-private sector partnerships.

Where does Sweden stand today?

Sweden has a relatively high degree of computer literacy and has worked actively to strengthen the general level of IT security over the past ten years. Thus, in international comparisons of risks linked to IT threats, Sweden does relatively well. Our critical infrastructure, on the other hand, is not constructed to resist attacks, in either cyberspace or the real world, from an entity with the resources of a state. There is still much to do.

The primary objective of FOI's work on IT security has been to raise awareness and introduce protections against the simplest types of attack. IT security has been a small area of research relative to the speed of developments in the IT field more generally. Maintaining attention on security aspects can be a challenge in a period of such rapid development. There is a major need for more advanced research.

Changes in the global situation in recent years have led Sweden to begin to reconstruct its civil defence, and the concept of total defence has gained new relevance. The societal change associated with the Internet has occurred since Sweden last implemented total defence and the new total defence set-up will have to include defences against digital threats.

The roles for managing digital threats need to be clarified. Whose job is it to put out fires on the Internet? If foreign military flights violate Sweden's borders, the Swedish Armed Forces scramble their own aircraft to intercept them. If a German freight train loaded with chemicals derails outside Stenungsund, it is the police and the fire department that deal with it. In the Internet world it is different, not least because civil and military threats blur into each other.

Sweden's resilience against digital threats will depend on how everyone in society collaborates. Collaboration already exists between the defence authorities and the crisis management system but must be developed further. In example, more explicit collaboration between the police and the military authorities must be forthcoming, and the opportunities for the armed forces to support the police must be expanded. In addition, civil suppliers of critical societal functions, such as mobile phone operators and banks, must be involved in planning for and managing threats. This is a major challenge for total defence.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
https://foi.se/en.html

Influence operations on the Internet constitute a clear threat to democracy and our political processes. It is obvious that during the construction of total defence we must also build competences and develop technologies to help understand and detect these attacks, to enable us to effectively oppose this type of subtle warfare. This type of external influence is already happening.

National and international regulation will be required to deal with digital threats. It will remain a challenge, however, to regulate such a rapidly changing area. At the same time, it will also be important to protect openness on the Internet. Sweden has a role to play in standing up for a type of openness that facilitates accountability. In the same way as there is a fire department to respond to fires that an individual cannot handle alone, maybe we need a force of volunteer IT technicians that has undergone training and is prepared to act in a crisis in a way that an individual system owner cannot when facing a major disturbance that it cannot handle alone. Does Sweden, like Estonia, need a digital home guard?

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
https://foi.se/en.html