OFFPRINT FROM *STRATEGIC OUTLOOK 8*

Cyber defence – skill needs practice

Tommy Gustafsson and David Lindahl

Since the turn of the millennium, cyber incidents and suspected cyber operations have had a profound impact on many countries and organisations. Sweden has a high degree of digitalisation of vital societal functions and the individuals who handle these systems daily play a key role in our total defence.1 It is therefore important to hold regular exercises for these people in how to handle cyber incidents. Currently, too few exercises are taking place, and it is also difficult to implement them realistically and pedagogically. Ensuring the national total defence capability requires relevant training environments, increased exercise volume, and research into training methodology.

Cyber operations

Cyberspace is an arena where both operational capabilities and doctrines have evolved significantly over the recent decades. It is an arena where the interests of military and civilian actors meet, and the threat from cyberattacks poses new challenges for Sweden's total defence. A conventional conflict is limited by geography; for an enemy to be able to strike against Sweden, it must first pass the border, through the protection provided by the Swedish Armed Forces. A cyber operation, i.e. activities in cyberspace perpetrated by a state to achieve military or political objectives, allows an attacker to strike against all the computers that are accessible for communication without the conventional defence forces being able to do anything about it.

As a consequence system administrators in civilian organisations risk being thrust into the front line of the conflict, in which case they will need the skills not only to ensure that systems are resilient enough but also skills to handle attacks.

Today, cyber operations are used on a regular basis for intelligence gathering, industrial espionage and sabotage. International conflicts have occurred wholly or partly in cyberspace. There are examples of cyber operations where nations have attacked civilian targets, both directly and indirectly, using proxy organisations such as hacker groups. During the war between Russia and Georgia in 2008, more than one-third of Georgia's internet was seriously disrupted, governmental communications were stopped, and the National Bank of Georgia was forced to shut down all computer services for 11 days.

The cyber arena is also used for various types of influence operations. Most influence operations seem to be focused on manipulating public opinion on a particular issue. However, there are cyber operations that may have been used to influence the strategic decisions of sovereign nations. One such example is the 2009 cyberattack against Kyrgyzstan while it was negotiating to host a NATO base on its territory.

It is difficult to limit the effects of cyber weapons, such as malicious code, and cyberattacks. In 2010, the Stuxnet cyber weapon went well beyond its intended targets in Iran, and seven years later the NotPetya attack not only disabled ten percent of Ukrainian computers, but also spread beyond the country's borders and became the world's most costly cyberattack to date. Overall, developments within the cyber arena show that a threat to Sweden's vital societal functions exists, even when Sweden is not the intended target of a particular attack.

[1] The total defence is the Swedish term for the civil defence organisations and the armed forces combined.

FOI Memo 6867
Project Nr I181103
Approved by Mike Winnerstig

October 2019

FOI

Cyber defence capability needs

Many cyber security frameworks and guidelines highlight the need for knowledge about threats and protective measures. Amongst other things, this knowledge is necessary to utilize the available resources in the right way, for instance by prioritising technical and administrative protective measures. Proactive measures are important and it is often the knowledge and actions of individual system administrators that determine if an incident occurs and whether or not its consequences become serious. A good way to create this knowledge is to participate in exercises. Exercises provide experience-based learning without having to deal with actual incidents. Through practice, system administrators become more skilled and the systems more secure.

Cyber exercises such as the Locked Shields and Crossed Swords exercises arranged in Estonia, and Cyber Czech in the Czech Republic, are used internationally to increase defence capabilities,. Arranging exercises is also in line with Sweden's national cyber security strategy from 2017, which amongst other things, states that 'Regular national and international training is a prerequisite for developing and evaluating structures to manage serious IT incidents...'.

> "Many organisations that carry out vital societal functions are unaware of their role in Sweden's total defence capability and therefore of the importance of their cyber security capability."

In addition to the level of knowledge of individual system administrators, collaboration has been shown to be a key factor for quickly and effectively managing advanced large-scale cyber incidents. When Estonia was attacked in 2007, it benefited greatly from a national collaboration established between system administrators from different organisations providing vital societal functions. Exercises are a way of establishing a foundation for this type of collaboration.

Enhancing the national capability

To enhance the Swedish national capability in the cyber area, there are three major challenges that need to be addressed: firstly, access to relevant training environments and scenarios; secondly, an increased number of exercises; and thirdly, research is needed to ensure that the right skills are properly taught.

In order to create relevant training environments and scenarios, considerable knowledge is needed not only of IT, but also of current cyberattacks. Furthermore, a pedagogical proficiency to develop exercises that convey the complexities involved in cyber incidents is needed. Ideally, exercises should be conducted in operational IT environments, but this is rarely possible since it might cause disruption in the very systems the participants strive to protect.

An alternative is to create a replica of the IT environment in question, but most organisations lack sufficient resources to prioritise setting up parallel IT environments. Even if the technical systems were copied, it would be very difficult to simulate the activities of the users, thus limiting the relevance of the scenarios. A 'quiet' network, where only the attackers and trainees are active, differs greatly from reality.

Another problem is that there is often a need for several iterations of an exercise before the pedagogical elements work optimally, and the rapid changes in the IT field means that exercise environments quickly become obsolete. Most organisations are too small to continuously develop training environments and scenarios.

There are some commercial initiatives available, but these have so far lacked relevant training environments for the total defence. Resources for developing in-house exercises must therefore still be set aside by the organisation that is planning to arrange them, which exacerbates the difficulties described above. In cases where the commercial initiatives are foreign-based, this entails a security problem from a total defence perspective. Overall, the difficulties involved in developing and maintaining training environments and scenarios, as well as the lack of relevant commercial alternatives, mean that an investment in the total defence in this field is needed.

Similar initiatives are already taking place in several countries, with prominent examples in Estonia and

Norway. These aim to strengthen the national cyber defence capability in each country and often include actors from the armed forces, civil authorities, actors in the vital societal functions and higher education institutions. This mix of participants ensures that the exercises are based on relevant technologies, real-life scenarios, and are sufficiently widespread to have a positive and long-lasting impact on national cyber defence capabilities. A key component of these initiatives is the establishment of a national cyber range, where exercises can be developed and implemented.

In collaboration with the Swedish Civil Contingencies Agency and the Swedish Armed Forces, FOI operates the Cyber Range And Training Environment (CRATE) facility, which is used in research projects as well as in exercise and course activities. It has now become an advanced cyber range and includes a comprehensive IT infrastructure, as well as a number of specially developed tools for developing and holding exercises. CRATE could provide a good basis for a Swedish national cyber range.

The challenge to increase exercise volume requires both greater awareness and better access to relevant cyber security exercises. Many organisations that carry out vital societal functions are unaware of their role in Sweden's total defence capability and therefore of the importance of their cyber security capability. They primarily design their security activities to manage operational disruptions and would probably not prioritise cyber security exercises, even if such exercises were available. Improving exercise opportunities alone without raising awareness would therefore not lead to increased exercise volume.

To address the challenge of ensuring that the right skills are properly taught, educational research in relation to cyber security is required. Even though Sweden, like many other countries, has conducted exercise and training activities for more than a decade, there has only been limited research in this field. Arranging exercises with a focus on the needs of the total defence appears to be a workable method, not least considering the effects this will have on future collaboration, but further research is required to substantiate this.

Other important research issues in the field include technology and method development in cyber ranges, methods for increasing the exercise volume as well as how exercises can be used to generate decision data for future research. International examples also show that a national cyber range can be used to contribute to skills provision in the longer term by allowing higher education institutions to utilise it in research and education.

By addressing the challenges of providing exercise environments, creating an increased exercise volume, and a knowledge expansion on these through research, Sweden's cyber defence capability, and thereby the total defence capability, can be enhanced to meet the challenges of the future.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Telephone: +46 8 5550 3000
www.foi.se