CYBER Defence and Cybersecurity in a Total Defence Context

A **Small State Perspective** on Modern and Future Conflict

by **Major General Inge Kampenes**
Norwegian Air Force
Commanding General
Norwegian Armed Forces Cyber Defence

ACROSS NATO, MEMBER states are modernizing and digitizing their militaries to ensure more efficient management and increased operative effects and interoperability within the Alliance. Through the implementation of modern information communications technology (ICT) and communications and information systems (CIS), our Allies aim to strengthen their capabilities, while retaining the technological edge that has served NATO and its Members since the Cold War. It also led to NATO being the strongest military alliance in the world, and the North Atlantic Region to be one of the most peaceful and stable regions in the world since the Second World War. Consequently, NATO has been able to contribute to peace and stability outside its primary sphere of interest. However, with digitization comes new threats and risks. Capabilities for offensive cyber operations are being developed in most, if not all, countries around the world, and cyberspace operations are seen by many as an area where the smaller nations are able to project force on a more even playing field with larger nations, unlike with the traditional operational domains of land, sea, and air.

In parallel with this development is the emergence of non-state players also developing capabilities for cyber operations. Whether criminal organizations, activists, or digital guns for hire, cyberspace is presently a complex and chaotic operational environment that is contested by a large number of potential threats, and it will continue to do so in the future. Throughout time, conflicts have always attracted various non-state players seeking to profit in one way or another from the chaos, uncertainty, and the confusion that an armed conflict brings on both in the political, judicial, and private sectors of a society in conflict. Through the introduction of the Internet, which disregards key operational factors such as time, distance, and geography, profiteering in various forms are likely to be an even bigger factor in future conflicts than it has been in the past.

As the ongoing COVID-19 pandemic has shown, there are globally active threats that emerge whenever a society is in a state of crisis, and there are few limits to the measures criminals and activists will take to profit on the misery and troubles of others.

The evolution of the cyberthreat will, to sum it up briefly, have a major impact on future military operations, be they on sover-

The Norwegian Armed Forces Cyber Security Centre at Jørstadmoen, Lillehammer. Photos by Anette Ask, Forsvaret.

eign territory or on foreign soil. The implementation of two new operational domains by NATO over the last five years, cyber and space, greatly enhance the complexity of military operations, planning, and the role of military leaders. Furthermore, the battlefield will have more complexities, with both military threat actors and other players sowing confusion in the areas of operation.

Defining Cyberspace

There are many definitions of cyberspace, and for this reason there is little point in arguing for or against all these definitions, or, God forbid, try to introduce another one. In order to keep it simple, and within the confines of what is agreed upon by most, cyberspace can easily be sorted into three key elements:

The first element is the devices and information producing equipment, whether it is mobile phones, digital radios, computers, or servers. These units produce, store, process and visualize or present information and constitute the machine interface, which is tangible and visible to the users.

The second element is the networks that tie the devices together, whether it is landlines, radio links, wireless transmissions, satellite communication, or the endless other ways in which to connect devices. In general, communication technology has little value unless the units are connected, and these connections are also significantly vulnerable since the connectivity is what entails most of the potential vulnerabilities to ICT and CIS. Simply put, one could obtain 100 per cent security if the computer were disconnected from power, if the network card was removed, and if it was encased in cement. But, then again, what remains of the computer would not be of any use.

The third element is the information, algorithms, and data that flow through the networks and between devices, laying the foundation for information exchange, and from which we get all the benefits of digitization.

> "The evolution of the **cyberthreat** will have a major impact on **future military operations**."

From a military operations view, each of these three elements of cyberspace is irrelevant in isolation. Indeed, any device is irrelevant unless it provides some benefit to operations. Similarly, networks in isolation give no real value to a commander, and the information in our networks and devices provide little or no

real benefit if it is simply stored somewhere. Hence, there is a clear interdependence between the devices, the networks, and the information and data. Finally, I should add a fourth element to cyberspace, which is the *effects* that all the other three elements have on operations.

When devices are working as they should, the networks are interconnected, and the flow of data is timely, accurate, and undisturbed, we get the desired and tangible effects on which our operations are dependent. Precision-guided fires, precise navigation, improved situational understanding, information superiority, the ability to exercise command and control, and the potential for joint and combined operations. This fourth element is important from two key perspectives; on the one hand these effects are the main reason why we invest in technology and digitization. On the other hand, these are also, in a shooting war, the effects that our opponents will seek to disrupt or degrade.

For an opponent in a conflict situation devices, networks and information will be attack vectors, but not the objective itself. The opponent targets the three first elements of cyberspace in order to gain advantage by disrupting our operational effects.

Operationalizing cyberspace:
The cyber technician students during an exercise.
Photo by Anette Ask, Forsvaret.

Complex Dependencies

Modern military forces have complicated digital value chains. This leaves us potentially more vulnerable to cyberattacks compared to a decade ago. Many nations, like Norway, have reduced the size of their armed forces and focused their resources and manpower on the sharp end of operations. This has led to a reduction in the size of the rear echelons of traditional military operations. Elements like heavy maintenance, logistics, medical facilities, and communications have, to a smaller or larger extent, been sourced to partners or economized out of the standing structures. This has been a natural thing to do in a period where the Alliance has been largely focused on out-of-area operations, while at the same time many nations have downsized their militaries. The focus has been on maintaining structures able to solve the current mission portfolio.

Additionally, the most advanced military equipment on the market today is so technically advanced that it is difficult, if not impossible, to maintain or refit without a close partnership with the producer. More sourcing is taking place across the nations than before as a result of such partnership agreements. This leads to more cost-efficient military organizations, but also increases the military dependencies on society at large and on the global marketplace with its complex value chains.

The Total Defence Complex in a Cyber Context

As a nation that long ago based its national defence concept on the idea of a total defence structure these complexities have long been part of Norwegian military operations. However, the realization of cyberspace as a conflict arena has brought these issues closer to the forefront.

There are mainly two factors that lead to cyber operations influencing the total defence construct compared to traditional operations.

Firstly, geographical distance is irrelevant as far as cyber operations is concerned. This means that you can launch an attack on a selected target from the other side of the globe without any significant warning.

The second factor is time, as an attack can cross the globe effectively in seconds. Undeniably, this places strain on the established readiness and response times for both civilian and military organizations.

Further complicating the total defence system is the fact that most civilian and governmental organizations depend a lot on digital services and ICT systems, while establishing security levels that are primarily dimensioned to address peace-time threat levels, that is mainly digital crime. The security levels vary significantly from depending on the organization, on what threats they perceive to be relevant at any given time, and on the resources available to prioritize to cyber security.

Lately, across the globe, we have seen that organizations spanning from health services to logistics and food production have been attacked by criminal groups, sometimes leading to significant disruption of services for shorter or longer periods.

From a military total defence concept perspective, we have to accept that corporate

cyber security quickly can turn into an operational risk and a threat to the mission should the total defence partners experience cyberattacks in crisis and war.

Addressing Vulnerability in Cyber Operations

The complexities of cyber operations generally mean that there will not be enough time to increase the security levels of partners at the start of a crisis or a conflict. One may use military assets to bolster the defence of certain partners, but there will never be enough resources to provide support to all members of the total defence construct.

In order to ensure a high level of security among total defence actors, it is necessary for the nations and the armed forces to be a demanding partner for the total defence community. Contracts, agreements, and guiding documents need to address cybersecurity and cyber defence as prerequisites, and the governments need to validate and ensure that commitment is adhered to.

Furthermore, there should be more information and intelligence sharing in order to ensure that relevant parties have a common situational awareness and risk awareness regarding cyberthreats. Such sharing must be in place in peace and bolstered in crisis and war.

Dependencies and vulnerabilities need to be mapped in order to ensure that both governmental institutions and the armed forces understand the operational risk properly. The aim is to retain an awareness of threats and risks for each respective mission.

With the dependencies and vulnerabilities in mind, we need to ensure that the operational plans prioritize operational centres of gravity, and that the centres where the threat of hostile activity is highest are given more military support.

Resources must be prioritized in time and space to ensure that critical assets in the operations plans are protected from degrading or sabotage of ICT and CIS tools and services.

Plans need to be in place should cyberattacks eventually succeed to ensure that redundancy and robustness measures compensate for loss or degrading of services that are part of the total defence of the nation.

The Cyberthreat Landscape of Modern Conflict

The cyberspace domain has led to new threats and risks for all military operations. It is, therefore, important that all military commanders consider this in their planning and execution of operations. While our nations continue to build important capabilities to deal with cyber operations, adversaries are building capabilities too. Criminals, activists and organized multinational criminal groups can cause significant damage to our nations, influence national economies, or severely impact sectors of society. We need to be prepared that all these groups will be part of future armed conflicts. Either as profiteers, as mercenary groups serving the intents of the involved nation states, or groups that benefit from the chaos and uncertainty of post-conflict societies.

With the cyberspace domain being able to influence both the physical, cognitive, and information dimensions of conflict, as well as the evolution of information activities through cyberspace, future conflicts are likely to be fought in a very complex operational environment that stretches far beyond military players.

BELOW, CLOCKWISE: Major General Inge Kampenes at a cyber security conference, photo by Anette Ask; during a visit to the Joint Warfare Centre (JWC), photo by JWC PAO, and while observing a winter exercise of the Norwegian Defence Cyber Academy, photo by Anette Ask.

"From a military **total defence concept** perspective, we have to accept that **corporate cyber security** quickly can turn into an **operational risk.**"