Band 3 / 2018

Tomorrow's Technology

A Double-Edged Sword

Anton Dengg (Ed.)

Schriftenreihe der
Landesverteidigungsakademie

Schriftenreihe der
Landesverteidigungsakademie

Anton Dengg (Ed.)

Tomorrow´s Technology

A Double-Edged Sword

3/2018
Vienna, March 2018

Imprint:

Copyright, Production, Publisher:
Republic of Austria / Federal Ministry of Defence
Rossauer Lände 1
1090 Vienna, Austria

Edited by:
National Defence Academy
Institute for Peace Support and Conflict Management
Stiftgasse 2a
1070 Vienna, Austria

Schriftenreihe der Landesverteidigungsakademie

March 2018
ISBN 978-3-903121-31-7

Printing:
ReproZ W 18-1248
Stiftgasse 2a
1070 Vienna

7 Outlook

Complexity, Systemic Risks and Converging Technologies[287]

Herbert Saurugg

This chapter will address *Complexity, Systemic Risks and Converging Technologies* from a different point of view to raise awareness regarding possible challenges in connection with Converging Technologies that might not currently be in the focus of security considerations.

Network Centric Warfare

I would like to start my considerations by looking back 15 years, when Network Centric Warfare (NCW) was also a big topic in the Austrian Armed Forces. The discussion centred around the question how to improve military capabilities with new technologies and the possibility to connect sensors, command and control systems and actors in a much better way than we could ever have done before.

What really happened

Not particularly to the Austrian Armed Forces, because we were luckily not engaged in major military conflicts. But let us take the US Armed Forces as an example, which were the major driving force behind Network Centric Warfare. In fact they were really successful by using this concept in military

[287] This article originally was written in 2016 as a contribution to this book, but was published in a slightly altered version on a later date in a blog http://www.herbert.saurugg.net/2016/blog/vernetzung-und-komplexitaet/complexity-systemic-risks-and-converging-technologies, accessed on 11 December 2017.

operations, such as in Iraq or in Afghanistan, at least at the beginning of these wars. But was this sustainable as well? Not really. The high-tech forces, especially the supply chains, were successfully targeted by enemy forces which caused major casualties and cost an enormous amount of money. This was done by simple but highly sophisticated low-cost techniques, like, for example, using mobile phones to build efficient roadside bombs. The so-called Islamic State succeeded in establishing itself and spreading, within a very short time, over a very large area; they did so by, amongst others, using modern technologies, like Social Media to recruit followers and broadcast propaganda. Moreover, mass migration from the former war theatres started, which also preoccupied the Austrian Armed Forces, but in a completely different way than we had thought before. So the primary military operations were very successful because of the use of new technologies and the concept of Network Centric Warfare, but it was not possible to bring peace and democracy to these countries, which had been the official reason for deploying military forces there.

The missing holistic approach and view

So my conclusion is that our preparations for Network Centric Warfare were important but were insufficient with regard to the overall topic. The focus had mainly been on hard military targets – which is the main task of military forces – but disregarded other major developments. And it had been assumed that enemy forces were not connected or not using systems similar to those of friendly forces. Looking back this was short-sighted and a wrong conclusion.

The focus had been on hard military targets but in reality, the enemy was weak and poorly organised, as we assume enemy forces to be. This current enemy is using new civil technologies with capabilities that the armed forces were dreaming of fifteen years ago, and still are. Everybody can communicate wirelessly worldwide by using GPS – originally a military system – to beat high-tech military forces that are always equipped with the

As we have already learnt, the main driving force for the developments mentioned was – and is – interconnectivity by easily available ICT (information and communication technology) and, therefore, the amount of available information. So the question is "Do we now have the capabilities to control information of hostile forces?", "Can we disrupt their information flow?", "Do we know what is going on?", and "Can we stop virtual support?" Not really. Even if the drone war of the US Forces is based on information gathering and the tracking of digital traces. But most other security forces do not have these capabilities.

Even if we handle this topic very carefully, these capabilities could also be misused (unintended side effects). However, we will not be successful by merely focussing on hard military targets and on solutions that were successful in the past. We also do not want mass surveillance, as for example, performed by NSA. The question is whether we really need this on a very large scale or whether it could also work on a small, focused scale, as described by the concept of Electronic Warfare. We should not throw the baby out with the bath water. So broader discussion and transparent decisions will be needed to answer these questions.[289]

Times of VUCA

This is also a good example for the fact that we live in so-called VUCA times', the acronym for volatility, uncertainty, complexity and ambiguity, which is directly connected to the increasing complexity caused by the ongoing man-made interconnectivity between everything. In particular, we are not used to dealing with ambiguity.[290]

[289] Ibid.
[290] Ibid

Transformation to Network Society

During the Industrial Age we had simple structures and clear hierarchies that worked very well most of the time. The ongoing transformation to the Network Age or Society will fundamentally change our life and societies. Considering ongoing developments, it is dangerous to be guided by the knowledge and experience of former times, even if past solutions were successful then.

One major challenge will be that the structures and thinking of the Industrial Age will not completely disappear; however, they will be increasingly losing in influence and importance. This will enhance the complexity as well as the challenges for those who have to keep up with the developments.

But where is the link to Converging Technologies now?

It is the transformation to a Network Society and the digitisation process that also leads to Converging Technologies and Emerging Risks. On the one hand, these developments lead to fast and far-reaching improvements and, on the other hand, this entails completely new challenges and risks including for the security sector. In our culture we are used to an *either-or way of thinking*, which will no longer enable us to tackle future developments in the right way. It may have worked more or less with the simple structures at the time of the Industrial Age, but it will not in complex Network Age structures. Therefore, we will need an 'as-well-as' way of thinking, in order to address reality and ambiguity as we can see it already on an almost daily basis. Other statements and points of view may sound easier and provide short and clear answers; however, in a complex environment they are often false and harmful in the long term perspective, considering, for example, the populist tendencies of our times. Populists have short and very simple answers to many unanswered questions, and

people believe them, even though we already know that they will not function and are dangerous for our societies.

Systemic risks

This will be similar developments in, and reactions to Converging Technologies. We often try to address new possible risks with methods that were successful in the past, which, however, can hardly tackle the increasing interconnectivity and complexity. So the rise of systemic risks is hardly noticed. Systemic risks are characterised by a high degree of interconnectivity and interdependence and missing range limitation. Cascading effects are possible. Because of the complexity and feedback loops, there are no simple cause-and-effect chains and the triggers as well as the impact are systematically underestimated by the responsible persons and organisations.

From my point of view, the most dangerous short-term systemic risk is contained within the Europe-wide electrical power system. If this system failed, the effects could have major cascading and disruptive effects on the entire European society. Also the Network Centric Warfare example showed developments that were underestimated. Therefore, systemic risks are the root of X-Events, which John Casti described in this book.

What does complexity mean?[291]

Complexity is already a part of everyday language use, even if different meanings are often associated with it, such as opacity, uncertainty, dynamic, and so on. To address complexity in a very short way, it can be also described by some typical characteristics:

[291] Cg. Ibd.

- Changing system properties because of feedback-loops, and therefore the possibility of emerging new system properties. For example, oxygen and hydrogen are flammable gases; those two elements combined with aqua lead to a liquid that disguises a fire. Even if we knew the nature of the gases, we would not be able to foresee the nature of the new element.
- This also causes non-linearity, where our approved risk-management systems inevitably fail and predictions are difficult or impossible. They may work, as usually, work for a time, but within one moment the system's behaviour could change completely.
- Interconnectivity leads to an increasing dynamic (faster and faster …) because the possibilities with regard to the system's behaviour are increasing.
- This also leads to irreversibility (no way back) and the impossibility of reconstructing the causes or restarting at a well-known point. Take a creature as an example of a complex system: you cannot cut creatures into well-structured pieces, analyse them and put them together again. It will not work as will not for all complex (living) systems. This only works with complicated (inanimate) systems (machines).
- Another very well-known characteristic is that small causes could lead to large effects ('butterfly effect'). A minor problem in the link of a supply chain could bring down the whole system/production, as we have seen recently.
- Yet another characteristic that is often underestimated are delayed and long-term effects. Especially in our very short-term oriented economy. The figures are related to quartiles. We know that apparent short-term solutions often have a negative impact on a long-term view and that long-term success often requires the acceptance of short-term disadvantages. Take asbestos as an example of long-term effects. For years it had been considered a miracle material with great qualities, until people learned that it has

negative long-term side-effects and causes cancer. Now it has to be removed in compliance with high safety requirements and at high cost. Imagine what this could mean in terms of GN-technologies. It will not be possible to remove this parts because of the size of the material. As described by John Casti, an X-Event could be the consequence.

What challenges are we facing?

First, we have to know that in nature there are only complex, open systems. But they are new on a technical level, especially the increasing interdependences (vulnerabilities). We are still used to dealing with linear simple machines instead of complexity, mainly due to a lack of education and training. Especially in the education system we often still train and teach in a way that was appropriate for the Industrial Age, which is hardly what is needed in the upcoming Network Age; thinking in black and white is too simple.

Lack of knowledge and systemic thinking

There are of course improvements but, in general, they cannot keep up with the fast technological developments. Even though there are people who have the necessary knowledge to develop these emerging and converting technologies, most of them do not, including those who should, for example people working for public authorities or regulatory bodies who protect public interests. In particular, administrative bodies are often still organised according to old hierarchical structures that are hardly able to cope with quickly changing 'VUCA developments'. Not to mention that often interconnected special knowledge and fast reaction is needed. Today nobody is able to know everything anymore and therefore we have to arrange more flexible ad-hoc networks and interaction among different experts in order to address complex dynamic challenges. We are increasingly establishing and improving interconnections between technical

systems, but the necessary interconnection between people and organisations to cope with unintended side effects is lagging behind. This leads to gaps due to complexity, which implicate systemic risks and danger of X-events!

Cyberspace

I would like to give you another example. Are we prepared for the challenges connected to Cyberspace? At the moment we are mainly focusing on cybercrime and data theft. But this is just the beginning. We should be much more aware and worried about our Critical Infrastructures (CI). Yes, we have established Critical Infrastructure Protection, Cyber Security and Cyber Defence. But protection is not enough because perfect security does not exist anywhere.

Therefore, we have to rethink our system design, because the way we have organised not only our infrastructure but also our reaction capabilities is not appropriate for handling X-events. We are not prepared for dealing with major disruptions in our infrastructure either. And with the increasing interconnectivity and interdependence, especially within our infrastructures, the danger of far-reaching X-Events is growing.

We still have different 'silos' from those we had in the past. So we have a Critical Infrastructure Protection and Cyber Security where the police is responsible. Military forces should be responsible for Cyber Defence. But if Cyber Security fails and cascading effects bring down infrastructures, there will be no second line of defence where Cyber Defence could be successful. The only task will be to clean up the mess on a very basic level.

So what does this mean in the context of Converging Technologies?

The main question is "What are we talking about? Are we talking about possible military developments, which are of course there, but mainly concentrated on a small scale, like Network Centric Warfare?"

Or should we focus more on possible other realities that should concern us more, as they are relevant for the security sector and the society? For example, on drones over Critical Infrastructures that could lead to major cascading effects, or drones that hit aeroplanes and bring them down; or already existing biological invaders that could lead to an environmental collapse? And how much more easily could this happen if GNR-technologies are used? Therefore, we have to recall complexity and some of its characteristics: small causes, large effects, delay/long-term effects, irreversibility, increasing dynamic and so on.

Possible consequences for the security sector

The main question is "Who is responsible?" However, it remains unanswered because there has been no major event until now. But this is not a good way of dealing with uncertainty. Military forces are principally qualified to think ahead and to address security-related developments before they escalate.

This requires us to be vigilant, to have early warning systems and to be attentive with regard to weak signals because developments always follow an s-curve: very slowly and on a low level at the beginning. But at one point, the development increases in an exponential way, and soon a critical point will be reached with no way back. If the weak signals are neglected, you can hardly follow the developments. And we really have a poor understanding of exponential developments.

The only chance to keep up with 'VUCA developments' and GNR is to stay flexible and agile and not to resort to former military core skills. The challenges will not come only from the known side or the enemy. Therefore, we need an 'as-well-as' way of thinking: we require both and we need to look at both sides of the coin. So the security sector will be confronted with an increasing number of requirements.

Of course, the question remains "Who is responsible now?" Nobody and everybody. These topics are new to our society and therefore a new way of thinking and acting will be called for. Less than we did until now because an increasing technical connectivity also needs a way of thinking that takes into account the interconnectedness of systems, not only in the military forces but also within the whole security sector.

Learning from nature: 'Small is beautiful'

Therefore, we should also learn more from nature, which can look back to a very long history and development. Only successful structures have survived. We often neglect the so-called 'silent witnesses', those who did not survive and cannot be found in history books. One major structure that succeeded is 'small is beautiful'.

- Small structures are more flexible and robust against strokes (asymmetry).
- People are more resilient in small structures.
- You cannot prevent the development, but early warning is an important part of navigation and we have to prepare to cope with uncertainty and with major incidents/disruptions (X-events).
- It is all about communication and knowledge. If people and decision-makers know the challenges, they can react to, and prepare for crisis/disruption or change the path.

- Communication in the security area will be a main driving force in increasing people's resilience and their capability to act in case of uncertainty and after X-Events.
- Understanding the problem is half of the solution.

So we are moving on a very narrow path. The border line between benefits and risks is very thin. One main question therefore is "Are we mature enough?"

The good news at the end:

- Near future X-Events will most likely not be triggered by GNR – even if we cannot give a guarantee.
- But we should consider major temporary infrastructure collapses and social unrest, because there have been/are many weak signals which have been hardly noticed until now.
- We also have to be attentive to weak signals in other areas – like GNR.
- And we should learn more from history and transfer this knowledge into the future; although history never repeats itself, there are similarities we should search for.

This book will just be the start when it comes to increasing our increase awareness of new challenges for the security sector with respect to Converging Technologies and Emerging Risks.