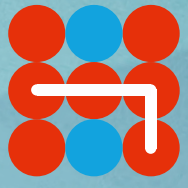
RESEARCH AND ANALYSIS

Hybrid CoE Strategic Analysis 21

MARCH 2020

Cyber power is changing the concept of war

JOSEF SCHROEFL



Hybrid CoE

Hybrid CoE Strategic Analysis is typically a short paper (around 2,000 words) written by academic and research community experts. Strategic Analyses are based on long-term research experience, or on current or completed research projects. The idea behind the Strategic Analysis papers is to enhance understanding of different phenomena in the realm of hybrid threats. They do not present direct recommendations but aim to explain processes and identify gaps in knowledge and understanding, as well as highlight trends and future challenges. Each Strategic Analysis paper includes a literature list for further reading. Topics are related to Hybrid CoE's work in all of its main functions: training and exercises, communities of interest (hybrid influencing; strategy and defence; and vulnerabilities and resilience) as well as research and analysis.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-36-6
ISSN 2670-2282

March 2020

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

Cyber power is changing the concept of war

> *"We are at a crossroads when it comes to determining whether cyber should be compared with strategic weapons, and the destruction it causes with conventional war. If so, cyber should be tightly controlled, international law should take a stand on it such as a UN Security Council confirmation, and cyber diplomacy should be added to the diplomacy domain. On the other hand, should cyber be viewed as an operational or tactical capability available to all commanders? In both cases, the question is how to build a credible deterrence strategy to convince potential attackers that any attack would indeed be comparable to a declaration of war, even if cyber weapons are not viewed as Weapons of Mass Destruction but largely as Weapons of Mass Disruption (to use a phrase from the early days of cyber warfare theory)."* – writes Josef Schroefl, deputy director of the Community of Interest on Strategy and Defence at the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Imagine a scenario where multiple hostile cyber attacks start targeting our governmental, financial and industrial systems. The main target is NATO allied navies, even if at this point the real target is unclear. There are widespread power and internet outages impacting all critical sectors throughout Europe and Northern America. Allied forces around the world discover system outages ranging from sporadic reboots to "blue screens of death" for propulsion systems, radar, air traffic control systems and command and control networks affecting both classified and unclassified systems. It seems that the allied cyber defence forces were caught off guard. The attacker takes advantage of decades of priming, testing and capability-building. The cyber Blitzkrieg[1] has begun.

In this kind of scenario, cyber forces are likely to be overwhelmed. The responsibility for defending and, more importantly, restoring critical services might fall to private-sector IT and cybersecurity personnel.

With less than 16,000[2] cyber troops[3] in NATO and the EU, immature and untested tactics, techniques and procedures and no standard equipment designated for operators, commanders will find it difficult to recover from cyber-attacks by a determined attacker.

A first strike cyber Blitzkrieg that spreads across military and non-military sectors is a worrying scenario. Yet a scenario it remains, since we have not yet experienced an actual cyber Blitzkrieg in real life.[4]

1 Seen as a military strategy that is intended to prevent a conflict from escalating into a full-blown war and to achieve this through a rapid operational victory; spearheaded by a dense concentration of combined arms, breaking through the opponent's line of defence with short, fast, powerful attacks and then dislocating the defenders, using speed and surprise to encircle them. Through the deployment of combined arms in manoeuvre warfare, Blitzkrieg attempts to unbalance the target by making it difficult for it to respond to the continuously changing front, then defeating it in a decisive battle of annihilation if necessary.
2 The figure is the result of counting cyber troops from NATO and EU member states, according to the "Military Balance 2019", IISS, 2019.
3 In recent years, many states have integrated a cyber command into their armed forces. One of their tasks is to train cyber soldiers serving within cyber forces, better known as cyber troops, to fulfill the whole orchestration of cyber-defence tasks.
4 However, hundreds of smaller attacks against critical infrastructure have taken place across the world, and it is worth pointing out that cyber-attacks are a common occurrence in many critical infrastructure branches.

Cyber as a part of the landscape of hybrid threats

The nature of a national security threat has not changed fundamentally, but **cyberspace has opened up a whole new domain to be considered in conflict and war scenarios, and has provided a new delivery mechanism that can increase the speed, stealth, precision, diffusion, and power of an attack.**

The cyber domain and activity in cyberspace do not automatically constitute a hybrid threat. In the landscape of hybrid threats, cyber is only one domain in which harmful activity can take place. Cyber interference consists of operations by state or non-state actors conducted in cyberspace. If this activity targets critical infrastructure, for instance, by cyber means to achieve political/military aims alongside other activity by an outside hostile actor – we have hybrid action. Cyber interference, in its priming phase, can effectively spy on and manipulate electronic and information systems. At this juncture, it would be premature to talk in terms of waging war. It is not possible at this point to know whether the activity will escalate into war. However, as hybrid activity blurs the real aims and goals of the activity, it might force us to make hasty and poor decisions.

Cyberwarfare

Cyberwarfare refers to the new highly technical forms of warfare in the information age, which are based on the extensive use of computers and software, electronization and networking of almost all military and civilian areas. The intensity of these operations, their "success" in terms of the disruption and denial of IT services, computer programs and underlying networks, as well as in terms of disinformation and defacement, and lastly their political and/or strategic goals point to their characterization as cyber "warfare". According to professor and security expert S-D Bachmann, "Cyber warfare passes the threshold of other cyber activities such as hacking, spamming and phishing". If this type of cyberwarfare is combined with cyber activity that takes the form of confrontation in and around cyberspace, with resources primarily in the field of information technology, one is experiencing cyber warfare with hybrid characteristics.

In a cyberwar, attacking militaries would most likely exploit the ubiquity of cyberspace and global connectivity to conduct a full range of cyber-attacks against the target's national critical infrastructures and strategic assets on their home soil, deep behind the front lines of battle.[5] The possible success highlights how in the era of hybrid threats the enemy is penetrating our social and political space to exploit cultural seams – moving behind our backs instead of opting for direct confrontation.

The source of the intrusion or attack is very often anonymous. In cyberspace, the attribution of offensive actions can be obscured more easily. Its ubiquitous and unpredictable characteristics have changed the way in which war is waged and battles are fought. **The anonymous nature of cyber-attacks will complicate and perhaps even prevent traditional risk mitigation such as deterrence and the threat of retaliation. If this is achieved, the strategic objectives can be reached with relatively little effort.**

This may mean that virtually any future kinetic war will be accompanied by cyber strikes to perform a hybrid orchestration of attacks (i.e. in multiple domains, covertly, in a coordinated manner, etc.).

Even though there is no concrete example of a full-scale cyberwar, at least not yet, examples exist of how cyber can be used as a part of warfare activity:

1) **The first category of cyber-attacks would be conducted as part of a broader effort to disable the target's weaponry and to disrupt strategic/military C2 systems.** This was demonstrated in 2007 when the Syrian air defence was disabled by a cyber-attack before the Israeli air force destroyed an alleged Syrian nuclear reactor. There is also an indication that

5 See also Kurt Einzinger: "Cyber Warfare 2.0 - The Undertow of the Internet" in Schroefl/Rajaee/Muhr: "Hybrid and Cyber War as a consequence of asymmetry", p. 127 ff.

the Iranian military launched heavy cyber-attacks before they attacked the US military base in Iraq, in the aftermath of the January 8, 2020 strike that killed Iranian General Qasem Soleimani, in order to disable American aircraft and drone navigation systems.[6]

2) **The second category of cyber-attacks would be aimed at the target's ability and willingness to wage war for an extended period of time.** This is directed therefore not only towards the military but the whole society. The attack would be likely to include the target's financial sector, energy sector, industry, and national morale. This was the case in 2007 when IT attacks virtually and literally "crashed" Estonia's internet infrastructure.[7] This gives potential targets a sense of their own vulnerability.

Stopping potential attackers: Deterrence

The assumption has been that cyber warfare is more likely to reduce death and destruction compared with conventional (kinetic) warfare. The threat pertaining to the cyber warfare scenario painted at the beginning of this article is relatively small, since many states and especially hostile non-state actors still lack the capabilities to inflict much harm. It is still unclear whether cyber should be approached as a strategic weapon (such as nuclear capability). **We are at a crossroads when it comes to determining whether cyber should be compared with strategic weapons, and the destruction it causes with conventional war. If so, it should be tightly controlled, international law should take a stand on it such as a UN security council confirmation, and cyber diplomacy should be added to the diplomacy domain. Or should cyber be viewed as an operational or tactical capability available to all commanders? In both cases, the question is how to build a credible deterrence strategy to convince potential attackers that any attack would indeed be comparable to a declaration of war, even if cyber weapons are not viewed as Weapons of Mass Destruction but largely as Weapons of Mass Disruption (to use a phrase from the early days of cyber warfare theory).** The question at present is whether weapons of mass disruption can still cause physical destruction not directly but as a follow-up impact. For example, if cities are without electricity for a prolonged period, that could result in a greater number of deaths than would otherwise occur.

In order to deter, you need to build credible cyber capabilities, and let potential attackers know about these capabilities. The best example of this procedure is the minor US attack that occurred in June 2019 against the Russian power grid, when the US "mined" the power grid in plain sight.[8] The US simply let Russia know that it was in their systems, and that it could also escalate its attacks. As such, the operation was purely strategic and did not do any harm. **The strategic and diplomatic rationale for the operation is likely to be underestimated amid the predominant focus on the legal aspects of cyber diplomacy. One of the main deterrence aspects that should be linked to cyber is deterrence by demonstration, in the sense that deterrence requires the demonstration of responsive and available capabilities.**

These and other operations have given rise to an emerging order of an awkward strategic stability linked to cyber capabilities, and this stability has guaranteed that, despite all possibilities, a major cyber war between the great powers has not yet taken place. **However, a noteworthy aspect is that small states, especially those at the margins of the great powers, can be targeted due to the great power competition. Given the difficulties of defending against such attacks and the improbability of retaliation, a major question for small states is how to increase the costs (both operational and financial) for the great powers.**

6 See https://www.bbc.com/news/world-middle-east-51051826 (23-01-20), but also https://en.radiofarda.com/a/iran-disabled-us-monitoring-systems-during-missile-attack-irgc-commander-claims-/30368664.html (23-01-20).
7 In 2009, K. Goloskokov, head of the Russian youth group Nashi, claimed responsibility for the attacks https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313 (08-02-20).
8 See https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html (23-01-20).

The future of cyber forces

Cyber forces are only a decade old and the war fighting experience of these forces varies considerably and is generally limited in scope and/or complexity. **Cyber power integrated into a broad campaign during the execution of a series of battles or engagements as a part of great power competition is likely to be very different from neutralizing adversary cyber forces that are using cyberspace as a part of the landscape of hybrid threats. This means, for example, conducting espionage as a part of priming, or achieving limited military objectives as a part of any destabilization operations.**

This is an evolutionary process, beginning with an expansion of the way in which the armed forces perceive cyberspace. It might also be evolutionary in terms of the way in which war fighting is seen. **Cyberspace is more accurately described as warfare against every processor and every piece of software on the battlefield. The decade or more of research and targeting that near-peer adversaries have conducted into allied systems and software will have undoubtedly yielded hundreds of cyber targets across the battlespace**. As operators in all military domains understand and react to cyber threats to systems (seen as the military IoT), cyber forces will be looked upon to help defend propulsion and weapon systems (military operational technology (OT) systems) and will become integrated with the traditional military domains – land, air and sea. This will also drive the demand for cyber forces to provide commanders with offensive cyber options for similar adversary systems across the battlespace.[9] However, the military alone cannot tackle the problem.

We need to strive to make cyber relevant and meaningful for every domain from both the military and the civilian perspective. An analogous model drawn from military thinking might be undersea warfare that is understood by submariners, ship operators and aviators working in coordination. **In the era of hybrid threats, cyber touches upon so many different domains that are beyond military planning and that are often even completely under the jurisdiction of local-level administration. Moreover, some of the best capabilities for detecting, deterring and recovering from cyber interference and operations belong to the private sector. This means that effective deterrence and counter-action has to be carried out in coordination with local, state and military planning as well as with the private sector.**

9 The author would like to thank Rear Admiral (ret) William Leigher (USN) for his assistance in reviewing this paper and in creating the cyber warfare scenario. Thanks are also due to Director Teija Tiilikainen and my colleague Hanna Smith for their help with editing and shaping this paper.

Author
Colonel **Josef Schroefl**, PhD, is the Deputy Director, Community of Interest on Strategy and Defence at the European Centre of Excellence for Countering Hybrid Threats. He started his career in the Austrian Armed Forces in 1982 and has worked since then in various areas of the military, including several UN tours within UNDOF to Syria, and commanding the honourable 4th Battalion "Hoch- und Deutschmeister", founded in 1530. Since 2006 he has served in the Austrian Ministry of Defence as Senior Staff Officer heading "Comprehensive Approach", "Hybrid threats" and "Cyber Security/ Cyber Defence".


Hybrid CoE