CSS
ETH Zürich

What it Takes to Develop a Military Cyber-Force

States often struggle to develop a military cyber-force, as the time and resources required for an effective capability are much greater than often appreciated.

By Max Smeets

In late 2016, several leaders of the US intelligence community estimated that more than 30 countries are in the process of developing "offensive cyber attack capabilities."[1] This number has steadily increased, with a wide range of countries – including the United Arab Emirates, Nigeria, and Vietnam – announcing their establishment of a military cyber command since. Despite this proliferation, there is still little understanding of the requirements to effectively operationalize a military cyber command.

In *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, I analyze the difficulties that states face in this area. The purpose of this policy brief is to highlight several key aspects of offensive capability development.

Key Points

- Offensive cyber capability development encompasses five key elements: people, exploits, tools, infrastructure, and organization.
- The most important element of developing an offensive cyber capability concerns the recruitment, training, and retention of personnel.
- There are both benefits and risks to organizational integration between military and intelligence.
- There is a tension between establishing standard operating procedures to carry out complex routine operations and maintaining individual flexibility.

Conceptualizing Cyber Capability Development

The nature of offensive cyber capabilities continues to be frequently misrepresented. We often hear that "cyber weapons" can be sold or that states have an "arsenal of cyber weapons." Yet, it is often unclear what a "cyber weapon" refers to. Consider a case of an actor gaining access to a computer system through social engineering and removing files or directories. What is the weapon in this scenario? An offensive cyber capability refers to an actor's ability to conduct cyber operations. Cyber operations are a set of linked activities – bringing together technology, skill, and organizational processes – spanning target acquisition to payload delivery and beyond.

We can break down a cyber command's challenges of building an offensive cyber capability into five categories. The first are the *people* required to run an effective cyber operation. Second, a state developing an offensive cyber capability will need to think about how it can *exploit* vulnerabilities in computer systems to gain, escalate, and maintain access. The third requirement to develop an offensive cyber capability is the *toolbox*, a set of computer programs used to create, debug, maintain, or otherwise support other programs or

applications. Tools normally form part of a larger "toolchain" to allow for the (consecutive) execution to perform an offensive cyber operation. Fourth, there are infrastructure requirements. *Infrastructure* can be broadly defined as the processes, structures, and facilities needed to pull off an offensive cyber operation. It can be split into two categories: control infrastructure and preparatory infrastructure. Control infrastructure refers to processes directly used to run an operation. This is also the type of infrastructure that is generally "burned down" after a (failed) operation. This type of infrastructure can include domain names of phishing sites, leaked email addresses, or other abused technologies. Preparatory infrastructure concerns a set of processes that are used to put oneself in a state of readiness to conduct cyber operations. Rarely will an attacker throw away this infrastructure after an operation. The final elements refer to the *organizational* processes to effectively operate.

"Cyber Warrior in Switzerland" created by Artificial Intelligence generator Dalle 2 Mini on huggingface.co.

People, People, and People

To develop an effective offensive cyber capacity, the first element – the recruitment, retention, and training of people – is the most important. A widespread view in business management is that as the cognitive skills required for a job increase, people – rather than technology – become more important. These "thought jobs," as Daniel Pink calls them, require greater problem-solving skills and creative thinking, which means that businesses can only be successful if they cultivate a culture that prioritizes the human element. For aspiring cyber powers, this is true for more than just technical experts.

Of course, a military cyber command needs vulnerability analysts, or bug hunters. These employees search for software vulnerabilities. They also need developers, operators, testers, and system administrators to successfully execute an operation, and make sure that capabilities are reliably developed, deployed, maintained, and tested.

But building an offensive cyber capability also requires a more comprehensive workforce. First, frontline assistance is required to support the activities of operators and developers. This can include activities such as registering accounts or buying capabilities from private companies. Second, a military or intelligence organization with the best cyber-force in the world is bound to fail without strategic guidance. Operational or tactical success does not equal strategic victory. An operation may be perfectly executed and rely on flawless code, but this does not automatically lead to mission success. For example, US Cyber Command may successfully wipe data off the server of an Iranian oil company without actually securing any change in Iranian foreign policy. An organization can only function if there is a clear understanding of how the available means will achieve the desired ends. An important task of strategists is to coordinate activities with other military units and partner states. They are also involved in selecting target packages, although a separate position is often created for "targeteers." The targeteers nominate targets, assess collateral damage, manage deconfliction, and help with the planning of the operational process.

Any military or civilian agency conducting cyber operations as part of a government with a legal framework will also deal with an army of lawyers. These legal experts will be involved in training, advising, and monitoring. Compliance with the law of war, the law of armed conflict, and any other legal mandates requires legal training operators, developers, and systems administrators to prevent violations. Legal experts provide planning support as they advise, review, and monitor operational plans. For example, in the planning of US Cyber Command's 2016 Operation Glowing Symphony, which sought to disrupt and deny the Islamic State of Iraq and the Levant's (ISIL) Internet usage, these experts helped to specify the notification plan, mission checklist, and authorization process.

Embedding legal experts at the various stages of a cyber operation is hard. Indeed, it likely requires numerous critical conversations with the leadership and operational

teams to ensure that they sufficiently understand what is being proposed before they can give approval. Also, the way certain operations are executed makes legal vetting harder. For example, in the case of self-propagating malware like Stuxnet deployed against the uranium enrichment centrifuges in Natanz, Iran, once you commit, it is difficult to go back.

A diverse group of technical analysts is then needed to process information during and after operations. Non-technical analysts are essential, too, particularly for understanding how people in the target network will respond to a cyber operation. This requires analysts with specific knowledge about the country, culture, or target organization. There is also the need for remote personnel. As security researcher and former NSA employee Charlie Miller put it, "Cyberwar is still aided by humans being[s] located around the world and performing covert actions."[2] In the case of the Stuxnet attacks, for example, a Dutch mole, posing as a mechanic, helped the United States and Israel collect intelligence about Iranian nuclear centrifuges that was used to update and install the virus.

Finally, a cyber command needs administrators for human resourcing, liaising with other relevant domestic and international institutions, and speaking to the media. As Jamie Collier observed, "[G]one are the days when spy agencies did not officially exist" and kept "their personnel and activities guarded surreptitiously away from the public view."[3] Communication can help to overcome public skepticism. This applies not just to intelligence agencies, but to some degree also to military cyber commands, especially when their mission set is expanding and concerns about escalation, norms deterioration, or allied friction are growing. In addition, being more public facing may help for recruitment purposes in a highly competitive job market.

Further Reading

Max Smeets, ***No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*** (London/Oxford: Hurst Publishers & Oxford University Press, 2022).

Matthew Monte, ***Network Attacks and Exploitation: A Framework*** (New Jersey: Wiley, 2015).
Provides an excellent primer on how we should conceptualize cyber operations.

Herbert S. Lin / Amy Zegart (eds.), ***Bytes, Bombs, and Spies: The Strategic Dimensions of Offenisve Cyber Operations*** (Washington: Brookings Institution Press, 2018).
The volume includes diverse perspectives on the strategic role of cyber operations.

Integrating Military and Intelligence

While people are the most important element when it comes to developing offensive cyber capacity, organizational characteristics and processes have a major impact on what people can achieve. An essential inter-organizational aspect concerns the effective integration of intelligence and military priorities.[4] Organizational integration can come in many shapes and forms: appointing the same director for the intelligence services as for the command carrying out military activities; people moving from intelligence unit to a military unit and vice versa; and setting up the same training program to those running espionage operations and those conducting cyber effect operations – i.e. operations with the aim to disrupt, deny, degrade, and/or destroy.

One benefit of organizational integration is that it could allow for an efficient allocation of resources in that the same processes or tasks are not unnecessarily replicated. It can put staff to better use, as integration frees up further resources for specialization. This means task complexity can be increased as tasks can be divided based on who is most proficient in the process. Tools and infrastructure can also be used more efficiently. For example, integration makes it easier to reuse parts of code from a different operation to save time and resources.

In addition, we know from the organizational management literature that organizational integration can stimulate the transfer of knowledge. Empirical evidence suggests that interconnected organizations such as franchises hold a comparative advantage over their more autonomous counterparts due to the ability to transfer knowledge across their constituent parts. For example, a restaurant may put a new dish on the menu that was successfully served at its sister restaurant located in a different part of town.

The knowledge to perform offensive cyber comes in two forms: explicit and tacit. Organizational integration is not a necessary condition to transfer explicit knowledge. For example, a government could set up a course to teach hackers how different elements of an Industrial Control System work. The tacit knowledge component is more difficult to articulate – and cannot be taught in the same manner. As Michael Polanyi stated, "we can know more than we can tell."[5] This refers to knowledge embedded in a hacker's experience or a military organization's (implicit) operational processes. Forms of organizational integration, however, potentially allow for the transfer of this type of knowledge as well.

There are also several risks attached to organizational integration. Most notably, too much overlap between tools used for intelligence and military operations increases the risk of exposure and makes attribution easier. The proverb

"don't put all your eggs in one basket" not only applies to a financial investment strategy, it also holds for offensive cyber operations: It makes sense for states to delink their intelligence capabilities from their warfare capabilities – especially when the organization (occasionally) utilizes custom tools.

Organizational Routine Versus Individual Flexibility

In developing organizational processes, there can also be tension between establishing standard operating procedures to carry out complex routine operations and maintaining individual flexibility. Standard operating procedures to promote routines are important for any organization. One benefit of routines is that they provide stability, which in turn leads to predictability. In the cyber environment – sometimes described as a domain of uncertainty – predictability of actions is certainly a welcome asset.

At the same time, an offensive cyber organization must also foster an environment in which operators can depart from routine and nimbly adapt their actions to stay ahead of their adversaries. As Martin Libicki observed, there is no "forced entry" when it comes to offensive cyber operations.[6] "If someone has gotten into a system from the outside, it is because that someone has persuaded the system to do what its users did not really want done and what its designers believed they had built the system to prevent," Libicki argued. Thus, to ensure repeated success, one must find different ways to fool a system administrator. Repetition of an established organizational routine is likely to be insufficient when conducting military cyber operations: innovation is equally important.

There is no easy way to resolve this dilemma as few of the conventional mechanisms used to encourage creative behavior can be applied to a government organization seeking to achieve cyber effects. A common form of encouragement is to reward risk-takers in the organization. Conversely, military cyber organizations (and intelligence agencies) need also be risk-averse and cautious. It is essential for "cyber soldiers" to stick to the rules to avoid escalation and possible violation of the laws of armed conflict, just as it is for more traditional soldiers. Despite the need for unpredictable and deceptive responses, military cyber organizations cannot simply try things out and see what happens, given the potential of butterfly effects in cyberspace – small changes in code that can escalate into large-scale crises.

Similarly, to stimulate creativity, private companies often grant individuals autonomy. The underlying management logic for granting personal autonomy was perhaps most famously spelled out (and radically implemented) by Brazilian entrepreneur Ricardo Semler: Let employees decide how to get something done, and they will naturally find the best way to do it. This is less straightforward for military cyber organization. For cyber operations, while outcomes are important, precisely how the job gets done is equally relevant. After all, the modus operandi of one cyber operation may greatly affect the effectiveness of other operations.

A New Game Afoot?

Most scholarship on the dynamics of cyber has focused on whether cyber effect operations can produce strategic advantages or be influenced by norms. Yet, implicit in this debate is the assumption that states can participate in cyber conflict, that they have crossed the barriers to entry. *No Shortcuts* challenges this assumption and explains that, for many states, the barriers of entry are much higher than often perceived to be.

Selected sources

1. James R. Clapper / Marcel Lettre / Michael S. Rogers, "Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States," *U.S. Senate,* 05.01.2017.
2. Charlie Miller, "DEF CON 18 – Charlie Miller – Kim Jong-il and Me: How to Build a Cyber Army to Defeat the U.S.," youtube.com, 2013.
3. Jamie Collier, "Getting Intelligence Agencies to Adapt to Life out of the Shadows," cfr.org/blog, 2017.
4. Also see: Max Smeets, "Integrating offensive cyber capabilities: meaning, dilemmas, and assessment," *Defense Studies* 18:4 (2018), 395–410.
5. Michael Polanyi, *The Tacit Dimension* (London: Routledge, 1967).
6. Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 16.

Max Smeets is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich.

Policy Perspectives is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy.

Series Editor: Brian G. Carlson
Issue Editor: Boas Lieberherr
Layout: Miriam Dahinden-Ganzoni

Feedback welcome: PolicyPerspectives@sipo.gess.ethz.ch
More issues and free online subscription:
css.ethz.ch/en/publications/css-policy-perspectives

Most recent editions:
Russia's War and the Global Nuclear Order (10/6)
Sicherheitsordnung nach Moskaus Ukraine-Invasion (10/5)
The War Against Ukraine Shapes NATO's Future (10/4)
Goodbye Cyberwar: Ukraine as Reality Check (10/3)
Ceasefire Monitoring and Verification Technology (10/2)
Cyberneutrality: Discouraging Collateral Damage (10/1)

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000553756