Offensive Cyber Capabilities are Needed Because of Deterrence

Jarno Limnéll

Abstact

Within the next couple of years, the world will experience more intentionally executed and demonstrated cyber attacks. Simultaneously, the development of offensive cyber weapons will become fiercer and publicly more acceptable. As different actors develop more sophisticated cyber capabilities and acquire experience in their use, the picture will grow more complicated and nuanced.

Keywords: Cyber, offensive, deterrence, attribution, credibility, weapons, cyber treaty.

Today, cyber capabilities are essential for the nation states and the armed forces that wish to be treated as credible actors. Cyberspace, the fifth dimension of warfare, has already become an important arena of world politics – especially, since the times of war and peace have been blurred and become the grey area we are currently living in. The nature of cyberreality (the blurring of peace and war) adds a dangerous new dimension of instability: future conflicts may become vague, without a clear beginning and end. Sometimes the actor may not even be conscious of being in conflict with someone, when unpleasant tangible things "just happen" all the time or just every once in a while. The digital world has become a domain where strategic advantage can either be lost or won.

We are Moving toward a Ubiquitous World

It is very important to understand that in the future the difference between kinetic and non-kinetic environments will become ever more blurred and that in many respects these environments will merge into one.[1] Almost everything will be digitally interconnected, and the cyber domain will expand and become more complex. This indicates that the possibilities and means to do things will broaden considerably and that the integration of the cyberworld with the physical world will give a new dimension to human life. Therefore, cyber should not be treated as a separate domain, but as one that is entwined with the physical space.

In military terms this means that modern warfare will demand effective use of cyber, kinetic, and combined cyber and kinetic means.[2] Cyberwar could be an additional domain in traditional warfare or a standalone approach to warfare – both are likely to occur. Cyber operations can be kinetic and/or non-kinetic. Boundaries between conventional and cyber operations are blurring, since cyber attacks begin to be used as a force multiplier in conventional operations.

[1] Jurvansuu 2011.

[2] See, as an example, Department of Defense Strategy for Operating in Cyberspace 2011.

It is also essential to bear in mind that cyber attacks can do things that conventional attacks cannot – with devastating and unprecedented effects.

Defence, Resilience and Offense

Even if we would like to think so, success in the cyber domain is not only a question of defence – at least, not for the nation states. Defence capabilities have to be as preventive as possible in order to reduce the effectiveness of the adversary´s – whoever it may be – cyber attack. However, despite the best defensive efforts, intrusions will occur. Therefore, one also has to be resilient in the cyber domain, that is, one has to have the ability to withstand attacks and failures, as well as to mitigate harm more than in other domains. The creation of cyber defence capabilities and resilience are pretty easy for the public to accept. Yet, these acts are not enough. Deterrence is also needed, that is, the capabilities and policies to convince the others not to launch a cyber attack against one. Deterrence will only be effective if one can build and demonstrate offensive cyber capabilities. To put this in a clear manner: offensive cyber capabilities are an essential element for the nation-states to succeed in their current and future international and security policies.[3] Defence, resilience and offense all contribute to the country's overall ability to protect herself – one needs them all.

From Nuclear Deterrence to Cyber Deterrence

The ambiguities of cyber deterrence contrast starkly with the clarities of nuclear deterrence. In the Cold War nuclear realm, attack attribution was not a problem; the prospect of battle damage was clear; the 1,000th bomb could be as powerful as the first one; counterforce was possible; there were no third parties to worry about; private firms were not expected to defend themselves; any hostile nuclear use crossed an acknowledged threshold; no higher levels of war existed; and both sides always had a lot to lose.[4]

Deterrence theory was developed in the 1950s, primarily to address the new strategic challenges posed by nuclear weapons. During the Cold War, nuclear deterrence was able to keep the United States and the Soviet Union in check. Nuclear deterrence was the art of convincing the enemy not to take a specific action by threatening it with an intolerable punishment or an unacceptable failure. The theory has worked well.

Based on that logic, cyber deterrence should play a similar role in the digitalized world. However, anonymity, advantage of attacks, global reach and interconnectedness greatly reduce the efficiency of cyber deterrence. Simultaneously, there is a lot of suspicion and rumours travelling around: what kind of capabilities the others might have and how they are using them already?

In the kinetic world, it is much easier to evaluate the opponent's capabilities. It is quite easy to make a valid estimate on how many tanks, interceptors or submarines a country possesses. Countries also openly expose their arsenal, for example, in military parades, as

[3] Limnéll 2012.
[4] Libicki 2009.

well as their operational skills, for example, by organizing large military exercises. In the logic of deterrence, it is even more important to manifest force than to have real capabilities – yet the others have to know it.

Awareness Prevents Conflicts

Deterrence depends upon effective communication between the state and the entity it wishes to deter. One has to convince the others that if they attack, one has the capability and the capacity to do something about it. This is also the case in the cyber domain. If a country wants to be a credible actor in this domain, it should openly declare its offensive policy and expose its offensive capabilities. The policy acts as the rules for engagement. This is the trend some countries are already moving toward. For example, for the first time since the Second World War, Germany has publicly disclosed that it is developing offensive cyber weapons.[5] In addition, in the latest Cyber Strategy of the United States, offensive cyber policy is strongly emphasized, and it has been said in public that the US Defense Advanced Research Projects Agency (DARPA) is focusing its research on offensive cyber capabilities.[6] It has also been announced by many countries that a response to a cyber attack is not limited to the cyber domain, which is very understandable.

The world needs to start talking openly about offensive cyber capabilities and the readiness levels – just as we discuss missile arsenals, air force, submarine fleets, or doctrines. We talk about great military exercises taking place in the kinetic world, but there is very little public discussion on things happening in cyberspace. Today, countries are aware of and appreciate the kinetic capacities which the others have. This is one reason why there are so few on-going wars in the world. Awareness prevents conflicts – at least, between the nation states – and it raises the threshold for conducting an attack. The defence policy of many countries is based on this assumption – if you have and if you are able to expose strong enough military capability, the likelihood of being attacked decreases.

The Challenge of Attribution

Lately, there has been a lot of discussion about the problem of attribution, which differentiates the logic of warfare in the cyber domain from the other domains. Yes, attribution is hard because it lacks the obviousness of a kinetic attack and leaves no physical evidence. Attacks can also be masked or routed through the networks of another country. Even if one knows for sure that the attack came from a computer in a certain country, one cannot be sure that the government is behind it. It is hard to deter without being able to punish, and one cannot punish without knowing who is behind the attack. Moreover, hitting back to a wrong target weakens the logic of deterrence and also creates a new enemy. This allows totally new players enter the field of warfare which was formerly held solely by the nation states. These players are called terrorists. Cyber terrorists may take an advantage of the situation in which some or very little offensive capabilities exist.

[5] Leyden 2012.

[6] Nakashima 2012a.

Attribution is difficult, but it is not impossible.[7] It requires both technological solutions and diplomacy – and, in particular, wide international cooperation. Communication channels between countries should be created, and to be used when something extraordinary happens in the cyber domain. I am convinced that when countries start discussing their cyber capabilities more openly and admit the existence offensive strategies (which, in any case, are the reality), it will become politically easier to approach the touchy issues of rules and norms in the cyber domain in international cooperation. Where there is a will, there is a way.

At the same time, it has been interesting to notice that in some cases certain actors have willingly claimed the responsibility for conducting cyber attacks. If not doing so, the others would not know it and the actor in question could not take any political advantage of the attacks. This has been the case with Stuxnet. The U.S. government has unofficially admitted the attack in order to take credit for it – just before the presidential elections of 2012. By admitting Stuxnet,[8] the United States also pointed out that she was capable of and willing to use an advanced cyber weapon against an adversary. This is a strong message of deterrence.

Offensive Weaponry is Required for Credibility and Deterrence

Discussion on offensive cyber weaponry should begin. As emphasized, currently there is no credible status for the armed forces and the nation states without cyber capabilities – this includes the offensive capability. The arms race is on and accelerating, even if we would like to turn a blind eye to it. The most frantic contemporary race is about talented individuals. When it comes to the creation of cyber capabilities, the question is not about the number of people one employs but about the talent the employed have. The US, China, Russia and many other countries are actively recruiting promising hackers. So are, most likely, Al Qaeda and other organizations. The real cyber question is about the talent and about creating cyber capabilities with the help of the most talented individuals.

It is not very popular or even desirable to talk publicly about offensive cyber weaponry in most countries. However, it has become necessary to explain the logic of offensive cyber capabilities to the general public. Naturally, this has to be done in various ways in different countries due to cultural and national reasons. The reasons why countries are developing offensive weapons and why they need them can be summarized into the following four points.

First, if one wishes to be a *credible actor* both in the military battlefield and in world politics, one must have offensive capabilities – as one must have defensive capabilities and the ability to be resilient. One simply cannot have a credible cyber defence without offensive abilities.

Second, in order to achieve and *raise her deterrence*, one must possess offensive capabilities. The ability to act offensively includes a strong preventive message to the others – provided that they understand it and believe it. Offensive capabilities represent the key component of deterrence.

[7] Hunker, Hutchinson, Margulies 2008.

[8] Nakashima, Warrick 2012.

Third, offensive thinking and building offensive weaponry are vital in order to *create a strong and credible defence.* With just "defence thinking" one will not succeed. One has to have an understanding of how the attacker acts, and one should try to find all possible vulnerabilities in her own defence. It is also a matter of developing one's defensive potentials, testing the current defence and training one's forces. All this becomes much more efficient if one can test it with her own capabilities. Without the ability to act as an attacker, no country can build an effective and credible cyber defence.

Fourth, agility and the concept of operations for smart defence are reality in contemporary warfare for most countries. One will never achieve her objectives by just being defensive – regardless of how defensive her grand doctrine is. In some cases, as it has been in the past, attack is the best defence. One cannot stay in bunkers. Instead, one has to be an *active defender* and snatch the initiative when it is needed. Passive defence alone will not work. In short, when the lights go off how does one defend with kinetic weaponry against a non-kinetic adversary?

Disclosing Offensive Weaponry Becomes More Visible and Includes Great Risks

One of the biggest challenges and threats today is that countries are secretly developing and using their offensive cyber capabilities. The trend is very worrying. Offensive cyber weapons have already become so sophisticated that they are able to produce major disturbance, as well as paralyze societies´ critical infrastructure.

In every domain of warfare, there is the concept of deterrence which consists of real capabilities, doctrine and the others' awareness of one's capabilities. Merely talking about offensive cyber weapons in general terms, without revealing or even demonstrating these capabilities, will not advance deterrence very much.

Currently, cyberwarfare initiatives often follow the rules of guerrilla warfare. However, this will change soon. As the four-star General James Cartwright has said: "We've got to step up the game; we've got to talk about our offensive capabilities and train to them; to make them credible so that people know there's a penalty to this."[9] Just like with kinetic weapons, one's adversaries must know the weaponry possessed. In order to deter, the nation states must be able to show their capabilities without sacrificing the advantage that surprise may deliver – in defence and in offence.

In the next couple of years, the nation states will expose their offensive cyber capabilities more openly in order to enhance their deterrent effect. The states will demonstrate their capabilities by organizing exercises and simulations which will be openly reported. In addition, the effects of some offensive capabilities will be disclosed. However, most probably this will not be enough.

The nation states are "forced" to conduct cyber attacks in real situations and against real targets. This will mean attacks against terrorist or activist groups, industrial plants, or even

[9] Reuters 2011.

against other states. After conducting attacks, the nation states will claim the responsibility in order to increase their cyber deterrence. As an example, in May 2012 the US Secretary of State Hillary Clinton announced that the agency's specialists attacked sites related to Al Qaeda on which the organisation tried to recruit new members.[10] This was a strong political message of intent to use cyber weapons. It was a glimpse into the future of cyberwarfare – and it served to build credible deterrence.

Naturally, the question of using cyber weapons is controversial. When the nation states and other actors start to increase the use of offensive cyber capabilities, there is always the possibility of escalation. One event can quickly lead to another and an even greater conflict may arise – as the history has taught us. There is also the severe question of unexpected side effects which may occur when releasing cyber weapons. The end result could be, in the worst case, a total darkness of the unpredictable and interlinked digitalized world, even if that was not the original intention. Cyber deterrence within the area of operations may be very difficult to limit.

When the nation states are thinking about the creation of cyber deterrence, they face the aforementioned challenges. Something that is secret cannot be used as a deterrent. At the same time, there is too much detailed information on the weapons' capabilities available, which makes it easier for the adversaries to defend themselves against these weapons, for example, by blocking the vulnerabilities that the weapons exploit. Discussing or demonstrating cyber capabilities too openly would probably accelerate the cyber arms race even more and in ways that might be self-defeating. However, if the adversaries know that the digital infrastructure is resilient; that there is a credible threat detection and prevention system; and that there is a capability to conduct counterattacks, the deterrence is much more credible.

The Need for an International Cyber Treaty

It seems that the cyber domain turns all players offensive. So far, cyber operations have been interpreted as a "softer action", which makes the threshold of acceptability much lower than that of traditional military operations. In online strategy, offense dominates defence. In other words, it is more conducive to attackers than to defenders. This leads to new and complex dimensions in national security policy. There is a real need for the regulation of the digital battlefield agreed on a "Cyber Treaty." Cyber arms verification (identifying and measuring a given player´s offensive capability) is difficult, which increases the possibility of surprises in international relations. The absence of agreed or clear rules and norms, as well as the current imprecise knowledge of the ultimate cause-effect of cyber attacks can leave open ambiguity that leads to escalation. For now, there are no known or tested escalatory logics for a cyber battleground exchange. This begs the question of how far-flung militarization of the cyber domain we will testify.

[10] Axe 2012.

Civilians in the Front Lines of the Cyber Battle

It is important to understand that cyber deterrence cannot be undertaken by a government or an army alone. The general public must also be involved. Civilians are in the front lines of the cyber battle – every day. For example, if a significant number of home computers in a country have no firewall or anti-virus software installed, attackers will exploit these vulnerabilities each day to secretly take over and remotely operate thousands of computers hence turning them into botnets. This turns the nation into an adversary's offence capability and against itself.

The public is a very central point when creating cyber deterrence. It is not only about the importance of increasing the general knowledge about cyber security and the actions that must be done at the individual level. Everyone has a role when a country is trying to create more efficient cyber defence capabilities and to be a more resilient society. This may, in turn, create a totally new chapter in nation state economy and politics.

Countries are building offensive cyber capabilities and will use them more openly. If the general public does not understand the meaning of offense as part of defence, it is much more difficult to use them openly, that is, to strengthen the cyber deterrence. Thus, secret actions will continue, which will lead to much worse results. If the public understands the logic – and the seriousness – of creating offensive cyber weapons, the threshold to use these weapons will most probably decrease, because there will be an understanding of the devastating consequences. However, one will have her deterrence.

References

Axe, David (2012). "Clinton Goes Commando, Sells Diplomats as Shadow Warriors."", Wired 24.5.2012.
http://www.wired.com/dangerroom/2012/05/clinton-goes-commando/

Department of Defense Strategy for Operating in Cyberspace, 2011.
http://www.defense.gov/news/d20110714cyber.pdf

Hunker, Jeffrey; Hutchinson, Bob and Margulies, Jonathan. Role and Challenges for Sufficient Cyber-Attack Attribution, Institute for Information Infrastructure Protection, 2008.

Jurvansuu, Marko. Roadmap to a Ubiquitous World. VTT 2011.

Leyden, John. "Germany reveals secret tecnie soldier unit, new cyberweapons", 7.6.2012.
http://www.theregister.co.uk/2012/06/08/germany_cyber_offensive_capability/

Libicki, Martin C. Cyberdeterrence and Cyberwar, Project Air Force, RAND Corporation 2009.

Limnéll, Jarno. “Suomenkin osattava hyökätä verkossa”, Suomen Kuvalehti 30.9.2012.

Nakashima, Ellen. “With Plan X, Pentagon seeks to spread U.S. military might to cyberspace”, Washington Post, 30.5.2012.
http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html

Nakashima, Ellen and Warrick, Joby. “Stuxnet was work of U.S. and Israeli experts, officials say”, Washington Post, 2.6.2012.
http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Reuters, “Ex-U.S. general urges frank talk on cyber weapons”, 6.11.2011.
http://uk.reuters.com/article/2011/11/06/us-cyber-cartwright-idUKTRE7A514C20111106