Clingendael
Netherlands Institute of International Relations

Clingendael Alert

Sico van der Meer

DECEMBER 2019

The need for balancing offensive and defensive cyber operations

Source: U.S. Air Force / Master Sgt. Barry Loo

In November 2019, the head of the French national cyber security agency (ANSSI) commented on a cyber-attack that struck a public hospital in France. The cyber-attackers were identified as a Russian-based criminal hacking group. "The French law allows us to be active against the attacker, to neutralize it. We're not ruling it out," said the official.[1]

In May 2019, Israeli fighter jets bombed a building in Gaza, according to the Israeli air force because hackers linked to Hamas were using the building to prepare a cyber-attack against Israeli targets. No reports on victims of the bombing were released.[2]

[1] 'France not ruling out response to cyber-attack on hospital', *Bloomberg*, 28 November 2018.

[2] 'IDF says it thwarted a Hamas cyber-attack during weekend battle', *Times of Israel*, 5 May 2019.

And in 2018, the United States released its new Command Vision for US Cyber Command, which states that “We have learned we must stop attacks before they penetrate our cyber defences or impair our military forces; and through persistent, integrated operations, we can influence adversary behaviour and introduce uncertainty into their calculations.”[3] In other words: the US has decided that passive defence against cyber-attackers is no longer sufficient and has embarked upon what is called a strategy of ‘persistent engagement’. This entails that US cyber forces are allowed to infiltrate any computer network in other states pre-emptively, searching for planned attempts to conduct cyber-attacks against US targets, and to actively prevent these plans from being executed.

Diminishing restraint

Above are just a few examples of states that are becoming more offensive in defending their societies against cyber-attacks. This may not be a surprising development, considering the continuous increase in cyber-attacks globally and the apparent difficulties which states face in effectively defending against them.

More and more states are loosening their restraint in conducting offensive cyber operations because they conclude that offence may be the best defence. By preventing cyber-attacks before they occur or by retaliating quickly and forcefully after an attack, cyber-attackers may well be deterred from striking again.

Cycle of escalation

Offensive cyber operations may seem promising in deterring adversaries in the short term, but in the longer term they could cause a serious escalation of cyber conflict. If pre-emptive and retaliatory cyber activities become the ‘new norm’, more and more actors will follow this behaviour. The more actors pre-emptively infiltrate each other’s networks, the more the risk of chaos, (unintended) damage and escalation.

Pre-emptive cyber espionage aimed at detecting preparations for cyber-attacks may itself be considered a cyber-attack, thus starting an escalatory cycle of tit-for-tat retaliatory strikes. There is also a risk that intruders in networks will cause unintended damage while they are infiltrating these networks, or that other malign actors will closely monitor their hacking attempts to get entrance to the same networks. Thus, offensive cyber operations could start an unprecedented rise of cyber-attacks, resulting in global damage and chaos and maybe even in diminishing the reliability of and public trust in cyber technologies in general.

The risk that offensive cyber weapons are stolen and/or reused by malign actors is not imaginary either, as the global WannaCry and NotPetya ransomware-attacks of 2017 demonstrate: the basis for the malware was stolen from the US National Security Agency.[4]

Moreover, quick and forceful retaliation against cyber-attacks faces the problem of attribution. Although technical possibilities for the attribution of cyber-attacks are improving, it is often still difficult to attribute such attacks with one hundred percent certainty. So-called ‘false-flag’ operations may cause retaliatory attacks against an innocent party. Any actor facing retaliatory actions may respond by denying involvement in the original cyber-attack and by retaliating against the retaliatory actions as well, if only to emphasize its innocence (whether true or not). What if later, after time-consuming cyber forensic research, it appears that forceful retaliation was targeted at the wrong actor?

[3] *Achieve and maintain cyberspace superiority. Command vision for US Cyber Command*, 2018.

[4] ‘WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017’, *The Guardian*, 30 December 2017.

Improved attribution

Advocating restraint and the development of norms and rules in cyberspace, as many states do, seems to remain the most viable long-term strategy for a secure and stable cyber domain. An option to do so without neglecting the argument that new instruments are required to stop the increasing flood of cyber-attacks is to focus on improved attribution.

Instead of deterring cyber-attackers by starting offensive cyber operations, it would be better for global cyber security and stability to focus on another way to increase the costs for cyber-attackers. This can be accomplished by removing the 'cloak of invisibility' of the attackers by improving international cooperation in attribution, naming and shaming, and the sanctioning of states conducting, supporting, or not hindering cyber-attacks.

A precondition for improving attribution is to increase international cooperation, not only between states but also between governments and the private sector, including cybersecurity firms, tech companies and non-governmental organisations. Quick information exchange after large-scale cyber-attacks and better cooperation in forensic cyber capabilities are desired. This will enable more rapid and convincing attribution, putting the attackers in the spotlight, and in turn making effective retaliation more plausible.

Retaliation should not necessarily be done by counter-attacking, which risks starting a cycle of tit-for-tat cyber-attacks. Retaliation should preferably first start with other policy tools. Governments can respond in various ways before actual tit-for-tat counter-attacks, such as diplomatic protests, legal measures, and political or economic sanctions.[5]
This could well make cyber-attacks less cost- and risk-free for the attackers and decrease their number and scale, yet without the risk of creating even further chaos and damage in cyberspace by offensive cyber operations.

The Netherlands: defence or offence?

The Netherlands is very active in promoting restraint and the need for developing norms and rules in cyberspace. Dutch diplomats are investing a great deal in negotiations in the context of the United Nations (the UN Group of Governmental Experts and the UN Open-Ended Working Group), as well as in many multilateral or public-private settings. Examples are the Dutch-sponsored Global Commission on the Stability of Cyberspace (GCSC) and the Tallinn Manual Process.

Traditionally, the Dutch government focuses on defensive cyber policies, such as setting cyber security standards for vital infrastructure, public-private information exchange on cyber threats, and investing in cyber forensics to increase attribution possibilities. This, in turn, enables the naming and shaming and sanctioning of cyber-attackers.

Yet, even in a country such as the Netherlands offensive cyber operations are not a taboo. The Dutch intelligence services are known for having relatively large capabilities in cyber contra-espionage (think of infiltration into the networks of the Russian hacking organisation 'Cozy Bear' in 2016).[6] They also played a small role in the Stuxnet-attack on an Iranian nuclear facility in 2010, a clear case of cyber sabotage.[7]
Next to the intelligence services, the cyber unit of the Dutch armed forces, the Defence Cyber Command, is openly tasked by the government to develop offensive cyber weapons; there is no public information as to whether these weapons have ever been used.

[5] Sico van der Meer, *State-level responses to massive cyber-attacks. A policy toolbox*, Clingendael Policy Brief, December 2018.

[6] Huib Modderkolk, 'Dutch agencies provide crucial intel about Russia's interference in US elections', *Volkskrant*, 25 January 2018.

[7] Kim Zetter and Huib Modderkolk, 'Revealed: How a secret Dutch mole aided the US-Israeli Stuxnet cyberattack on Iran', *Yahoo News*, 2 September 2019.

Deliberate choice

It would be worthwhile to have more discussion on the desired balance between offensive and defensive cyber operations among policymakers and politicians (including Parliament). In order to effectively enhance a secure and stable cyberspace, the Netherlands should make a deliberate choice between following allied states such as the US in becoming more offensive, or, instead, showing that restraint is a viable way with more benefits in the long term. Not making a choice but doing both at the same time may harm the credibility of Dutch cyber policies overall.

Except for a small group of people directly involved in policy-making, there seems to be little discussion on balancing offensive and defensive cyber operations. Yet, the tension between advocating restraint and the need for norms and codes of conduct on the one hand, and following allies in adopting more offensive cyber policies, on the other, deserves more in-depth debate.

The Netherlands could seriously consider the option of investing more in attribution and retaliation in various ways, but not in offensive cyber capabilities for pre-emptive operations or quick and forceful retaliation.

Joining forces with as many state and non-state actors as possible that share the same perspective on long-term security and stability in cyberspace is recommendable. Shaping a broad coalition will increase the international visibility and impact of such a choice. Yet, such a deliberate choice needs to be preceded by a well-informed debate among policymakers and politicians.

About the Clingendael Institute
Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84

@clingendaelorg
The Clingendael Institute
The Clingendael Institute
Newsletter

About the author

Sico van der Meer is a Research Fellow at the Clingendael Institute. His research focuses on non-conventional weapons such as Weapons of Mass Destruction and cyber weapons from a strategic policy perspective.