Deterrence as a new military concept for cyber space

Inna Rodina
Nikita Degtyarev

Dual Master’s Degree Program in Nonproliferation Studies
Moscow, Fall 2019
Content

• Introduction;
• What is Cyber Deterrence?
• Obstacles in achieving cyber deterrence;
• Russia and Deterrence in Cyber Space;
• Conclusion;
• Bibliography.
INTRODUCTION


• The concept of cyber deterrence builds upon the strategy of cyber defence by incorporating both the ability to retaliate as well as the will to retaliate towards the cyber attacker.

• Cyber-attack as any action taken to undermine the functions of a computer network for a political or national security purpose.
What is Cyber Deterrence?

• Deterrence, in its broadest sense, means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks.
• Cyber deterrence seeks to dissuade the attacker from acting for fear of retaliation. It requires preparedness and a degree of retaliatory certainty, which is linked to having an offensive capability.
• Three pillars—a credible defense, the ability to retaliate and the will to retaliate.
OBSTACLES IN ACHIEVING CYBER DETERRENCE

• Problem of Attribution:
the difficulties to attribute with certainty cyber attacks to their authors undermine the very core of deterrence theory.

• Diminishing Capability to Retaliate:
cyber-attacks is a ‘one use weapon that is detrimental to achieving cyber deterrence as a successful retaliation may not be convincing if the attacker, who would perform the necessary security updates, believes it will be less vulnerable the next time around.
• Overcoming Potential Legal Issues
The unclear legal status of cyber warfare and retaliation in the cyber domain presents a challenge in enforcing the will to retaliate.

• Involvement of Non State Actors

• Avoiding Escalation:
difficulties in determining the outcome of the cyber retaliatory attacks and the uncertainties surrounding the reactions of the attacker, nations may choose to forego the option to conduct cyber retaliation. In consequence, this undermines the will to retaliation and compromises the strategy of cyber deterrence.
Russia and Deterrence in Cyber Space

- 2013, Russia was attacked with a cyber-weapon called “Sputnik.”
- 2016, Several Trojan horses in the IT infrastructure of Russia’s state, scientific, and defense institutions.
- 2017, The Washington Post: Barack Obama, when he was still president, ordered the U.S. National Security Agency to develop cyber-weapons against Russia as a response to Moscow’s supposed interference in the U.S. presidential race.
- Because of its participation in Middle East military operations, Russia has become seriously frustrating
- In 2016, Russian information resources had been attacked 70 million times.
Throughout Moscow, there are a handful of state research institutes where dozens of software specialists are developing and testing new cyber-defense systems: “Kvant” and “Voskhod,” the “Atlas” Science and Practice Center, and at an FSB engineering lab. Russia’s Defense Ministry also monitors vulnerabilities in cyber-defense technology.

Although, there has been much research on Russia’s recent cyber conduct, there has been very little focus on the Russian approach to cyber deterrence.

Andrei Krutskikh: "Those who wants to apply the concept of the deterrence theory to the cyber space must be aware that races on a mined filed are impossible."
• Deterrence in cyberspace is not possible and that entertaining the idea would be dangerous and destabilising.

• Five key objections can be identified in the Russian: 1. The impossibility of accurate attribution 2. Cyberattacks as a false pretext for war. 3. The risk to nuclear stability. 4. The unsuitability of deterrence to cyberspace. 5. The risk of an arms race.

• Oleg Demidov: «Cyberattacks against Russia will be answered but not necessarily in kind». 
USA and Deterrence in cyber space

The 2018 Department of Defense Cyber Strategy

New concepts:
• defending forward
• persistent engagement
• preparation of the battlefield
Defending forward

• Networks are no longer defended in one’s own perimeter or territory, but on the systems of potential attackers.
Persistent engagement

• Binding enemy forces by permanently exposing them to attacks by American hackers.

• It was applied during the Midterm Elections of 2018 against Russian “troll factory” (Internet Research Agency in St. Petersburg).
Preparation of the battlefield

• Opponent networks are to be penetrated in order to implant so-called back doors or logic bombs which can be exploited in future conflicts.
• This creates uncertainty, and attackers could refrain from serious cyber attacks.
How are other countries doing?

- Great Britain
- Germany
- China
- France
CONCLUSION

• Cyber deterrence is a difficult strategy to achieve. The obstacles such as problems in attribution, diminishing capability to retaliate, unnecessary escalation, involvement of non-state actors as well as the potential legal issues, make cyber deterrence a strategy that is difficult to achieve.

• An international regime of norms regulating state behaviour in cyberspace is necessary to complement cyber deterrence strategies and foster stability.
BIBLIOGRAPHY

- https://tass.com/politics/1001193
- Elena Chernenko, ‘Россия сделает все, чтобы не проиграть киберсоревнование’ Kommersant, 28 April 2016
Thank you for attention!