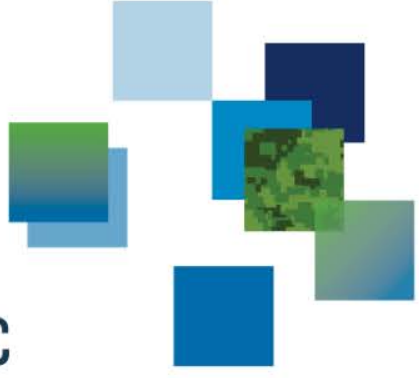
# An analytical wargaming approach to cyber deterrence

Abderrahmane Sokri, Ph.D.
Defence R&D Canada Centre for Operational Research and Analysis
Department of National Defence, Ottawa, Canada

The 13th NATO Operations Research and Analysis Conference
Ottawa, 7-9 October 2019



DRDC | RDDC

Canada

# Outline

- Cyber-deterrence
  - Forms of deterrence
  - Particularity of Cyber-deterrence
  - Credibility of Cyber-deterrence
- Ways to explore the Cyber-deterrence problem
  - Myopic approaches
  - Non-myopic approaches
- A wargaming approach
  - A possible scenario
  - A possible execution
  - Possible outcomes
- Way ahead

# Cyber-deterrence: Forms

- Deterrence is the persuasion/prevention from committing unwanted behaviour by fear of the consequences (DoD, 2008; Taipale, 2010)
- Deterrence manipulates the cost-benefit analysis of would-be attackers (Brantly, 2018; Wilner, 2017)
- **Deterrence by punishment** uses equivalent retaliation to increase the aggressor's perceived cost
  - Example from the physical world: The use of nuclear weapons
- **Deterrence by denial** uses impenetrability to reduce the aggressor's perceived benefits
  - Example from the physical world: Security mechanisms and higher walls around a critical infrastructure

# Cyber-deterrence: Particularity

- Deterrence is more complex than in physical domain
  - More non-state actors than nation-state actors
  - Digital attacks are highly dynamic and imperceptible to the human senses
  - Digital attacks go beyond all geographic and political boundaries
  - The attribution dilemma – Determining who to blame for an attack

    (Moisan and Gonzalez, 2017; Wilner, 2017)

# Cyber-deterrence: Credibility

- Classical theory of punitive deterrence involves a credible punishment
- The credibility of punishment depends on the blame attribution
- Deterrence by punishment may be very difficult and time-consuming in Cyberspace
- Deterrence by denial does not require the knowledge of potential attackers
- Deterrence by denial may be used to address this situation (Bordelon, 2017)

# Ways to explore the Cyber-deterrence problem

- **Myopic approaches**
  - Examples include decision-theoretic techniques and simultaneous games
  - Players make decisions in isolation
  - Players do not observe the outcome of previous actions before responding
  - A monotonic relationship between the investment level and the attacker's effort
  - The attacker will never be deterred because these approaches lack disclosure mechanisms
  - Literature: Gordon and Loeb (2002), Mayadunne and Park (2016)
- **Non-myopic approaches**
  - Examples include sequential games with disclosure mechanisms
  - Can solve the limitations of the myopic approaches
  - Literature: Cavusoglu et al. (2008); Sokri (Forthcoming)

# A wargaming approach: A possible scenario

We consider a security game between an attacker $a$ (the Red Team) and a defender $d$ (the Blue Team) in a cyberinfrastructure system.

| Variable | Definition |
|---|---|
| $T = \{t_1, t_2, \dots, t_n\}$ | A set of $n$ targets at risk of being attacked |
| $c(t_i), i = 1, 2, \dots n$ | The defender's cost if the target $t_i$ is successfully attacked |
| $S = \{s_1, s_2, \dots, s_m\}$ | A set of resources to cover the targets |
| $c(s_i), i = 1, 2, \dots m$ | The defender's cost associated with $s_i$ |
| $S = \{a_1, a_2, \dots, a_l\}$ | A set of $l$ types of attacks to attack the targets |
| $d(a_i), i = 1, 2, \dots l$ | The attacker's time to prepare the attack $a_i$ |
| $p(a_{ij}), i = 1, 2, \dots l$ | The probabilities of a successful attack on the target $t_j$ using $a_i$ |

# A wargaming approach: A possible execution

| | Blue Team | Red Team |
|---|---|---|
| **Objective** | To cover the maximum of targets with the minimum total cost | To conduct the maximum of successful attacks in the minimum time possible |
| **At each turn** | Publicly releases the level of investment | Reacts with a certain level of willingness-to-attack for each target (in terms of time) |
| **At the end** | A correlation coefficient will measure the strength of the relationship between the level of investment and the level of willingness-to-attack | |

# A wargaming approach: Possible outcomes

- At the end, a correlation coefficient will capture the potential correlation for each game.
- **Negative linear correlation**
  - When the investment is high, the effort should be low, and deterrence by denial would be effective
- **Positive linear correlation**
  - The investment would have an opposite effect
- **A value close to 0**
  - Deterrence by denial would be useless

# Way ahead

- The application of the model to a real-world cyber-security problem using real-life parameters,
- Analyzing the interaction between defenders and attackers in dynamic scenarios,
- Assessing the risk to the defender of a disclosure strategy,
- Including deception mechanisms to enhance security,


DRDC | RDDC
SCIENCE, TECHNOLOGY AND KNOWLEDGE
FOR CANADA'S DEFENCE AND SECURITY
SCIENCE, TECHNOLOGIE ET SAVOIR
POUR LA DÉFENSE ET LA SÉCURITÉ DU CANADA