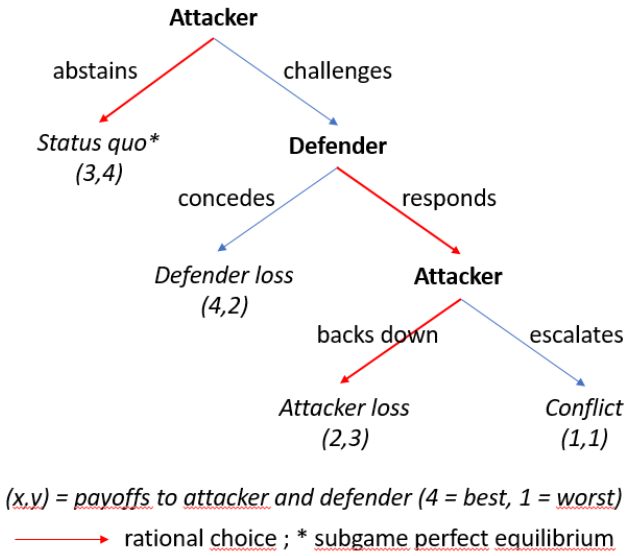
Cybersecurity: international cooperation requires reciprocity

Par Edouard Vidon, Céline Rochon

Cyberattacks have emerged as a major threat, including to global financial stability. By capturing the strategic interaction between cyber criminals and their targets, Game Theory provides valuable policy insights. It highlights the limitations and side effects of uncoordinated deterrence policies, and the importance of information sharing across public authorities. International cooperation is essential. The G7 is leading the way.

Figure 1: Game Theory in action: How deterrence can preserve the status quo



Note : adapted from Zagare, 2019

Potential losses from cyberattacks incurred by financial institutions have been estimated to range between 10% and 50% of their profits in a tail scenario (Lagarde, 2018). The magnitude of these numbers should be an alert for authorities in charge of financial stability. Yet cyber risk refers to a spectrum of threats extending well beyond the financial sector. In fact, successful cyberattacks against vital infrastructures such as hospitals, airports, and telecommunications could cause widespread disruptions involving large human and financial costs. Fortunately, the destructive impact of malicious attacks has so far been limited, but this should not lead to complacency.

When considering the challenge of cyber security, three distinct perspectives can be adopted:

- The strategic perspective sees cyberattacks in the context of interstate competition, or conflict, where cyberwarfare is increasingly used alongside conventional warfare, or even as a substitute for it.

- The operational perspective focuses on how to ensure the safety and continuity of specific information and communication technology (ICT) systems through the detection of threats, protection against attacks, as well as recovery and response after an incident. This is the main area of focus for financial regulators and supervisors.

- Finally, the global public good perspective looks into possible approaches to strengthen the international governance of cyber security.

Game theory offers valuable insights for each of these three viewpoints.

At the strategic level, defence policy experts have pointed out that states, as much as private companies, assert their jurisdiction over the cyberspace (Flournoy and Sulmeyer, 2018). State-sponsored cyberattacks have *de facto* been utilised as a vehicle for asymmetric belligerence. Classical deterrence theory emphasises the cost of conflict and the balance of power as key ingredients of stability. By contrast other recent approaches ("perfect deterrence" theory: Figure 1) stress the importance of the value of the status quo, and show that asymmetric power relationships can be very stable (Zagare, 2019). The main takeaway from this analysis is that negotiation with a potential cyber adversary should be "conditionally cooperative", i.e. threaten to respond in kind if the other state does not cooperate.

Deterrence efforts may deflect attacks toward weaker targets

Yet non-state actors also perpetrate cyber crime. In this respect, game-theoretic tools used to analyse counterterrorist policies (surveyed in Sandler and Arce, 2007) are of interest. The literature highlights the externalities involved in such policies. Deterrence actions taken to protect alternative potential targets (be it governments or businesses) can have negative externalities if such defensive efforts result in attacks being deflected toward weaker targets. In contrast, pre-emptive policy actions (e.g. seeking to neutralise criminal capabilities, or freezing their assets) have positive externalities benefiting all targets, but may result in free riding. Such public good provision faces the risk of insufficient collective action.

Figure 2 illustrates a simple cyber security coordination game: cooperative action means contributing to identifying and fixing security vulnerabilities. Non-cooperative behaviour corresponds to insufficient preventive action and possibly free riding on other actors' efforts to deploy adequate protection. However, the choice of actions also depends on the extent of information sharing that is expected from other players, and the associated costs and benefits. Two versions of this game can be considered:

- The prisoner's dilemma version, in which benefits from keeping private the information on threats drive non-cooperative behaviour, but result in a worse collective outcome.

- The ”stag hunt” version, in which the shared benefits from cyber resilience outweigh the benefits from keeping information private, but cooperative equilibrium still requires mutual trust.

Figure 2. Cybersecurity coordination game

Prisoner's dilemma:

Player A \ Player B	Cooperate	Defect
Cooperate	(2,2)	(0,3)
Defect	(3,0)	(1,1)*

Stag hunt:

Player A \ Player B	Cooperate	Defect
Cooperate	(3,3)*	(0,2)
Defect	(2,0)	(1,1)*

*(x,y) = payoffs to players A and B (3 = best, 0 = worst) ; * Nash equilibria*

At the operational level of cyber security implementation, ICT protection has also attracted the interest of game theorists. A typical example is the analysis of the attacker/defender dynamic interaction in a game originally applied to physical security: resource-constrained agents have to decide where to attack, and where to deploy protection (e.g. firewalls, etc.) respectively. An extensive survey (Do et al., 2017) illustrates the extent to which the game theory toolbox can be used to address challenges that range from denial of service attacks, to the interaction between the cyber and physical security of infrastructures.

The key message is that the management of cyber risks and potential security responses require an in-depth understanding of both incentives and vulnerabilities. Hence, convergence towards a suitably demanding regulation of cyber risk management should be promoted, with a view to avoiding regulatory arbitrage and ensuring sufficiently high standards.

How to encourage information sharing?

The problem of information sharing, which involves a trade-off between the benefits of shared intelligence and the protection of privileged information, deserves careful attention. Mechanism design theory suggests the use of auction-like schemes that incentivise truth telling. The difficulty of information sharing is particularly acute regarding the reporting of cyber incidents. In this regard, communication by impacted entities, including between governments, remains constrained by limited trust. Progress on that front would start with a common taxonomy of incidents, and convergence of existing regulatory reporting to obtain a more complete and reliable picture of evolving threats.

Table 1: Applying the Game Theory toolbox to address coordination issues

Sequence of interactions	Issues	Related game theory tools
Countries' reputation for reciprocity in a collective-action situation.	Credibility	Repeated games
Trust that all other participants are adhering to a reciprocity agreement.	Information asymmetries Moral hazard	Games with incomplete information
Extent of cooperation	Formation of stable coalitions	Coalition games
Net benefits	Sharing of gains and costs	Allocation mechanisms

Game theory tools (Table 1) highlight the difficulties of international cooperation. The failure of targeted businesses or nations to cooperate will encourage cyber attackers to search for the weaker links and targets. Last November, at the UNESCO Internet Governance Forum, France launched the "Paris call for Trust and Security in Cyberspace". This high-level declaration condemns malicious cyber activities in peacetime, and calls for the strengthening of international standards. In 2019, under the French presidency of the G7, cybersecurity for the financial sector has been identified as a priority of the Finance Track. A high-level international conference on "Cybersecurity: Coordinating efforts to protect the financial sector in the global economy" was organised by the Banque de France in May 2019. Ongoing work builds on "Fundamental elements" agreed upon in 2016 by the G7, with a focus on crisis management. Be it in the context of the G7 or beyond, the coalition of states willing to ensure a safe and open cyberspace seeks to share the benefits of cooperative actions and policies.