Maritime Cyber Risk Perception and Response

Kristen Kuhn[1], Salih Bicakci[2], and Siraj Ahmed Shaikh[1,3]

[1]Systems Security Group, Institute for Future Transport and Cities,
Coventry University, Coventry CV1 5FB, United Kingdom
[2] International Relations Department, Kadir Has University, Turkey
[3]Security, Risks Management and Conflict (SEGERICO) Research Group,
Universidad Nebrija, 28015, Spain

Abstract. Cyber risk perception and proportionate response to cyber attacks are important capabilities for NATO partners. Assessing perception and response is a challenge, particularly when capacity and level of preparedness is variable. Serious games are a tool to understand hybrid threat landscapes before a crisis. We examine threat perception and response with 68 cybersecurity experts with significant military/ public sector experience and variable cybersecurity expertise from 29 states, using scenarios that range over cyber incidents in the maritime domain. This game is a capacity building tool for NATO partners, trialled successfully in small setting. Effective assessment of cyber risk perception is done by calibrating risk in a group setting. As incident impact rose, group response favored private sector responsibility and visibility, but not directness or urgency. Our findings highlight the importance of planning for cyberspace operations in the maritime environment, and lay the foundation for future research on cyber risk perception as a intricate governing factor in incident response.

Keywords: Cybersecurity, Decision-making, Maritime, Risk perception

1 Introduction

In June 2020, The North Atlantic Treaty Organization (NATO) issued a statement [1] condemning cyber-attacks inflicted amidst the ongoing global health pandemic. About a month later, the UK National Cyber Security Centre also warned that Russia's APT29, a cyber threat actor known as "Cozy Bear," targeted Covid-19 vaccine researchers [2]. The assessment, they noted, was supported by key allies, including the Canadian Communication Security Establishment and the US National Security Agency.

Whereas one of the first steps of cyber incident response is to recognise an attack, NATO served as a collective body to release this information- over a month before states did so separately. This is an active demonstration of NATO's three core tasks, as defined in the 2010 Strategic Concept [3]: collective defense, crisis management and cooperative security.

It's not always that easy. The complexities of cybersecurity are a key factor in cyber incident response. Credible deterrence in cyberspace depends on capacity

and readiness to respond to cyber incidents. While it is individual states who decide to act, collective response is possible among states that share similar risk perception and a willingness to respond. By aligning to NATO, member states adopt a group risk culture and agree to support group response. However, this can be problematic when not all partners agree on cyber threats.

With respect to cyber operations, a starting point for effective incident response is to streamline cyber threats. Today, there is little to suggest shared situational awareness on cyber threats across NATO partners [4]. This has much to do with risk perception. In this context, our research is motivated by two questions: How can cyber risk perception be assessed effectively? Further, does work experience and cybersecurity expertise affect incident response?

To address these questions, this study develops a cybersecurity decision-making game. The game was conducted at a 2020 training course at the Centre of Excellence Defence Against Terrorism (COE-DAT). In groups, participants encountered three scenarios for which they ranked response.

We are particularly interested in maritime cyber risk, as maritime assets are complex and interdependent. As mentioned, the complexities of cybersecurity is a key factor in incident response. This is especially evident in traditional domains, such as maritime. NATO must have sufficient resources to adopt a defense posture that not only protects its borders but acts beyond its geography to ensure its security" [5].

A range of backgrounds factors are accounted for amongst the participants. This includes work experience and cybersecurity expertise. Existing research suggests that lack of experience leads to errors in cybersecurity decision-making. This is reinforced by a 2019 cybersecurity game [6], which found experienced subjects better learn the need for proactive decision-making through an iterative project. This study found experience to be positively related to effective decision-making. With respect to cybersecurity expertise, the fact alone that cyber risk actions tend to focus on technical measures [7] highlights the need for better cyber training, evidenced in the creation of the NCSC Boards Toolkit [8]. Likewise, it can be inferred that decision-makers are not tech-savvy and this is a wide issue as technical expertise is positively related to effective decision-making. The question, brought to light through this body of work, is if cyber incident response is affected by work experience and technical expertise of decision-makers.

This game is a capacity building tool for NATO partners, trialled successfully in small setting. It fosters planning for cyberspace operations in the maritime environment. Further, it addresses a key disconnect in crisis response, by sharpening technological skills and decision-making, when "NATO table-top exercises at the political strategic level are not sufficiently linked to the technical cyber level" [4]. We offer insights into how games can build capacity and the need for joint response.

The rest of this paper is organised as follows: Section 2 includes background information. Section 3 presents our methodology. Section 4 displays results and Section 5 includes a discussion of these results. Section 6 outlines our conclusions.

2 Background

2.1 The Centre of Excellence Defence against Terrorism

The Centre of Excellence Defence against Terrorism (COE-DAT) is one the oldest NATO centers, inaugurated in 2005. The Centre is composed of eight representatives from various nations to provide information on field-proven solutions and to challenge decision-makers on terrorism and counter terrorism.

COE-DAT acts to harmonize NATO resources and serves as the NATO Department Head in Education and Training. In addition, the Centre has to present a prospective outlook for the transformation of terrorism and its association with future security challenges to collective defense and a cooperative security approach. Since its inception, the Centre has collaborated with over 2503 guest lecturers, conducted more 200 courses and training activities, and hosted thousands participants from 108 countries.

This study was conducted during the "Terrorist use of Cyberspace Course" held from March 09-13, 2020 at COE-DAT in Ankara, Turkey. The primary goal of the course is to familiarize participants with key developments and the emerging threat landscape regarding terrorist use of cyber space and the utilization of this domain to support terrorist acts (including but not limited to fund-raising, recruitment, communication, propaganda, and training). It aims to cultivate participant understanding of national and international considerations for countering terrorist use of cyber space and to build a stakeholders' network around the issue.

The course is designed for military officers (OF-2/Captain and above) or civilian equivalents (police officers, experts) with minimal formal training in areas such as counter-terrorism and critical infrastructure protection. The course was open to select NATO individuals, NATO-partner countries and international organizations (such as the United Nations, European Union, and Organization for Security and Co-operation in Europe). The course included participants from 33 countries, most of whom took part in the cyber risk game to construct a better approach to the problems within hybrid nature of emerging security threats.

2.2 NATO cyber risk management in maritime security

In the post-Cold War era, the definition of threat and security has shifted and NATO has reorganized to respond to the emerging threat landscape. Increased globalization has also multiplied capacity of sea-bound trade: world-wide ship-borne trade quadrupled in volume since 1965 [9]. A significant portion of this naval traffic includes oil and gas tankers, which are critical for NATO operations and logistics. While the digital revolution has eased maritime navigation, it has also made the domain more accessible to illicit activity.

After 9/11, to sustain maritime security, NATO initiated Operation Active Endeavour (OAE) to counter terrorism operations in the eastern Mediterranean. Later in March 2003, the area covered by the operation was expanded to escort merchant ships in Strait of Gibraltar. During this endeavor, OAE forces hailed

over 88,000 ships, boarded more than 120 suspected ships and escorted nearly 500 ships [9]. Later, increasing threats to shipping such as piracy, hijacking and terrorism pushed NATO to reassess the situation at the 2006 Riga Summit [10].

From the NATO perspective, maritime security is deeply interwoven with energy security, economics, transportation, logistics, telecommunications, and beyond. On March 18, 2011, NATO published its Alliance Maritime Strategy that underlines the importance of the sea domain and maritime power. This strategy document also articulates the mission of the alliance to promote its values in this domain. Maritime security and its convergence with the digital infrastructure is also connected with ships, ports, naval vessels and various supportive devices. All these platforms became vulnerable to hostile activities. Naval vessels and interconnected systems are largely run by digital systems that carry cyber risks. The bridge systems, cargo handling and management systems, propulsion and machinery management and power control systems, access control systems, administrative systems and communication systems are vulnerable to cyber attacks.

Efforts have been made by NATO to address the shifting threat landscape. For instance, the Sea Centre of Excellence (CJOS COE) in Norfolk has inaugurated a maritime cybersecurity project to lead the development of a networked response to relevant threats and challenges [11]. NATO Allied Maritime Command (MARCOM) in the UK also closely focuses on the issue. MARCOM established a cyberspace division and organizes Maritime Cyberspace Security Conferences. Despite the increasing trend to understand maritime cybersecurity risks, the capabilities of adversaries are growing exponentially with limited effort.

As mentioned, NATO's three core tasks are: collective defense, crisis management and cooperative security [3]. While these remain valid, they are no longer sufficient: It is suggested [12] that "conserving stability might be a new responsibility for NATO to protect freedom in the global commons." That would include maintaining freedom of the seas and unimpeded passage through maritime choke-points; and curbing cyber operations that destabilize nations. International norms exist for much of the global commons, and NATO's task would be to consolidate and reinforce them. This must translate into a new set of missions and the alliance must find concrete ways to implement those norms.

NATO has made efforts to conserve stability through training, evidenced by the creation of the NATO Maritime Interdiction Operational Training Centre (NMIOTC). This center hosts cyber security conferences "to tackle the cyber security issues in the maritime environment" [13]. While NATO has made extensive efforts to add maritime cybersecurity to it agenda, protection of digital systems is only one dimension of the problem. A more significant issue remains the development of human factors in cybersecurity management and raising cyber awareness among employees and contractors. This research intends to comprehend the cyber risk perception of a sample group and provide a threshold for future study.

2.3 Cyber risk perception and response

Cybersecurity cannot be addressed through technology alone, and often requires strategic response from decision-makers [14]. While response classifications like the NIST Cybersecurity Framework [15] are employed, decision-makers must also rely on risk perception to respond to cyber incidents. Here, *risk* involves a state of uncertainty where some of the possibilities involve a loss, injury, catastrophe, or other undesirable outcome (i.e., something bad could happen) [16].

Risk perception is relevant to NATO military and civilian leadership because it influences their decision-making. It is acknowledged that, among other factors, perception rests on a foundation of experience [17]. Those who have not responded to a previous cyber-attack of similar nature have little reference, which is a contributing factor to poor performance. Subjectivity is another key challenge as risk is often formed on the basis of perception. *Perceived risk* is the estimated likelihood of occurrence [17], be it negative or positive. Indeed, these two aspects – positive and negative – make risky choice play a central role in decision-making under uncertainty [18].

One way to learn about perceived risk is looking at the response, whether that be to hypothetical scenarios or actual events. Errors in judgement by decision-makers, often due to incorrect risk perception, leads to disproportionate response, which can cause mistakes in resource allocation or incident escalation. In other words, gaps in perception of risk indicate gaps in capabilities to act [19]. The game based approach, used in this study, is demonstrated [6] to improve incident response through iterative learning.

Rather than the researcher being an expert, we work with a group of experts to streamline their risk perception against the group as whole. An advantage, unique to experienced or expert decision-makers is the idea of using a game to calibrate the group. That is, while games played by individuals aim at capacity building, games played by groups aim at communication and thus offer an internal qualitative measurement system. This is especially relevant when working with groups that have a wide range of backgrounds and factors amongst the participants, e.g. work experience, cybersecurity expertise. In this study, 47 participants from 29 countries are represented. This impacts risk perception: "Risk, after all, is a matter of perception and every society has not only a different perception of risk, but also a different threshold for risk" [19].

The participant group, as a unique sample, has its own risk culture, perception and threshold. We can explore participant backgrounds to learn more about the group, and why they might respond as they do to cyber incidents. While there is no right or wrong response, calibrated responses indicate effective assessment.

3 Methodology

3.1 Game design

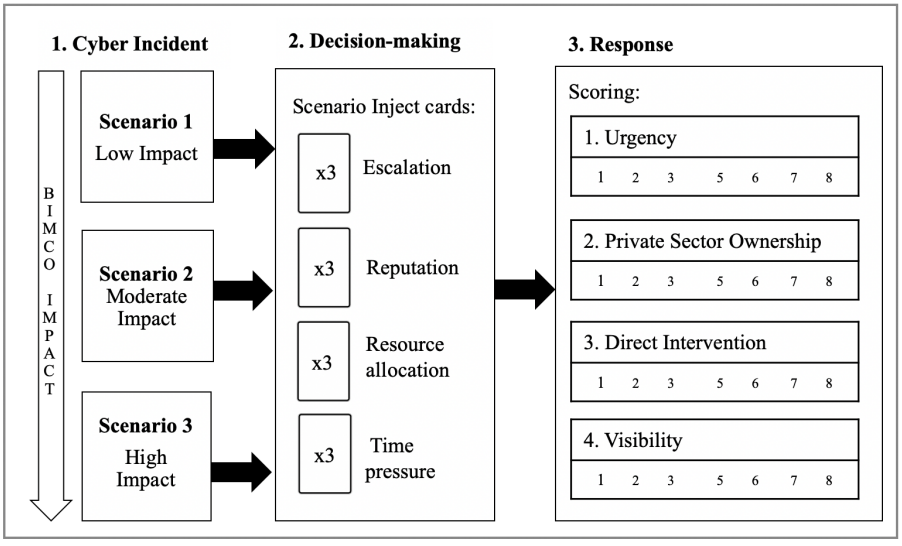
Built on earlier work [20], a cybersecurity decision-making game was conducted at a 2020 training course at COE-DAT in Turkey. There was a total of 47 participants in the game. The participants were divided into four random groups, each with participants from various countries, with mixed work experience and varied cybersecurity expertise. In groups, participants encountered three scenarios which they responded to by means of scenario inject cards to test decision-making. The game format is illustrated in Figure 1.

Game format includes three scenarios with distinct cyber incidents in the maritime domain. The scenarios escalate according to BIMCO Impact Levels [21]. For each scenario, participants respond to four scenario inject cards which are weighted according to the four response attributes to generate score (1-8) which is reported back to them at the end of the game. Results were analysed across groups.

3.2 Cyber incident

Participants assume the hypothetical role of "Cyber Incident Lead for the Maritime Response Unit of the National Security Council." As a security official, they advise the President on government and private sector cyber incident response, with specific regard to Arden Ocean Shipping (AOS), a fictional state-run container shipping company.

Fig. 1: Game format includes three scenarios with maritime cyber incidents.



Participants are presented with three escalating scenarios, summarised in Table 3. However, they are not aware of the escalation. This simulates reality, where decision-makers are often unaware of the severity of an event underway.

3.3 Decision-making

For each scenario, participants respond to four scenario inject cards, which represent situational changes to the scenario and require participants to make decisions. These were taken from previous research which explored decision-making aspects of a game [20]. Each scenario includes a card which corresponds to the four injects listed and defined in Table 1. Rather than an inject card itself, uncertainty is assumed to be an over-arching factor in the game. This is because uncertainty is a key component of a crisis [22] and is therefore an assumption in decision-making.

Table 1: The four scenario injects and their operational definition.

Inject	**Definition**
Escalation	Increased severity of incident.
Reputation	Shift in opinion of you or your company, causing loss or damage.
Resource allocation	Available resources to be distributed between two or more things.
Time pressure	Faster response is prompted.

3.4 Response

Four response attributes, based on those developed by Cyber 9/12 [23] and used in previous cybersecurity games [20], are shown in Table 2. Scoring was done by rating participant response on a scale (1-8), according to their reply to inject cards, where as each reply has a preassigned weight. Each inject type is paired once with an attribute type, so for example an escalation card may be paired with a situation that teases out visibility, and the response is then added to the final visibility score, whereas each card weighs two of eight points. This was done as an alternative to asking participants to simply rate their perceived response, to avoid confusion around application of terms.

Table 2: Response attributes, expressed as options, and operational definition.

Attribute	**Definition**
Direct intervention	Respond as involved actors, or ask intermediaries to intervene.
Visibility	Respond clearly/openly or ambiguously/behind closed doors.
Private sector ownership	Place responsibility on private or public sector.
Urgency	Choose an immediate or delayed response.

Table 3: Summary of the three escalating game scenarios, each with distinct cyber incidents which escalate to correspond with the BIMCO impact levels (low, moderate, high) detailed in Table 4.

Scenario (BIMCO Impact Level)
1. Unicorn of the Sea (Low)
AOS opens an arctic shipping route along Canada as opposed to Russia. The new AOS ice-breakers can access to ports previously isolated to trade. This is a sore point for the Canadian Inuit community, as the route crosses waters inhabited by narwhals. The Inuit have spoken out against AOS, claiming ships will disrupt narwhals and may push them to extinction. This issue gains international attention. AOS is reacting to a media storm- many posts from Russia. The shipping line opens with AOS Lunchbox departing from the Port of Iqaluit. But ship has not departed, as the PCT system which controls cranes that load cargo on the ship has been down for two hours. When they try to to access the system, dockworkers are redirected to the World-Wide Fund for Nature web-page with facts about the narwhal. Dockworkers cannot load the ship, and must work overtime until this is solved.
2. Parasite (Moderate)
AOS Peru reports that Peruvian police found a cocaine in the hull of AOS Dina embarking from Peru to Spain when they followed divers in the port, who planted it in a submerged ship compartment. However, when the ship sails the compartment where drugs were hidden is not submerged. The criminals have manipulated the ship OT systems which controls ballast, to lower the ship in the water to submerge the compartment, then raise her up- and repeat the process in the port of entry. This is hazardous to crew and cargo, as ballast grounds a ship. The cocaine was confiscated and the divers arrested. Police alerted the Spanish Guard for suspicious activity when the ship arrives. However, this group can enter, undetected, into the control systems of at least one AOS liner. Fines associated with transporting illegal substances are large in countries where AOS has a presence, and ships may be arrested in ports of entry.
3. Sitting Duck (High)
AOS Jasmine, a semi-autonomous commercial liner, is stranded in the Persian Gulf. Ground control in the UAE cannot turn on the propeller. The area is known for piracy, but no one has boarded the liner. Communication is being interfered with remotely, stranding the ship across a traffic lane. An Algerian oil tanker diverts from her course to avoid a collision with the liner, in turn hitting a fishing boat, killing nine. Responding to an SOS in domestic waters, Iranian military vessels search for survivors and redirect traffic. They also search nearby vessels, as they suspect one may be using a signal jamming device to remotely interfere with liner communication. Ship inspection grows more difficult as a traffic bottlenecks. The CEO of AOS receives an email from an unknown sender which demands the payment of $5 MM USD to a bitcoin account, in exchange for the control of AOS Jasmine.

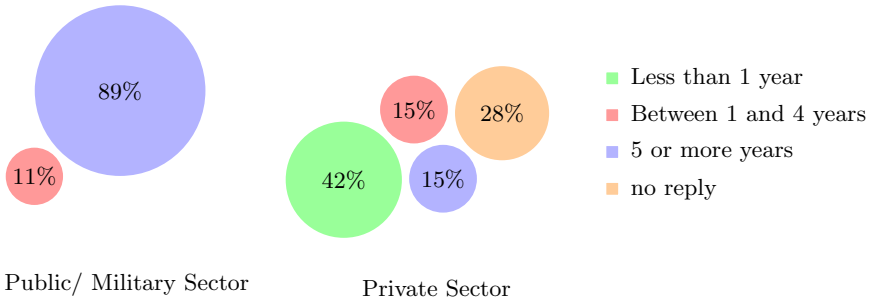
Source: BIMCO [21]

4 Results

4.1 Participants

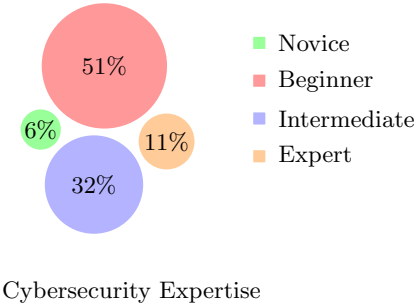
There was a total of 47 participants in the game. Prior to the exercise, each participant was asked about their work experience and cybersecurity expertise. Figure 2 shows the breakdown of the years spend in public and private sector. The group as a whole exhibited five or more years of experience in the public/military sector, and a mixed amount of private sector experience. It is interesting to note that while all participants reported their public/ military sector experience, over a fourth did not report their private sector experience.

Fig. 2: Participants' sector experience by percentage.



Participants were also asked to judge their cybersecurity expertise, as shown in Figure 3. The group as a whole exhibited moderate expertise, with the majority of participants rating themselves as beginner or intermediate. Fewer rated themselves either novice or expert, the two respective extremes on this spectrum. Therefore, we may infer general cybersecurity expertise among participants is calibrated.

Fig. 3: Participants cybersecurity expertise.



4.2 Effective assessment of risk perception

In response to the first research question, which explores how risk perception can be effectively assessed, we have elected incident classification as a starting point to calibrate risk in a group setting, i.e., among decision-makers.

Incident classification varies greatly, and for this study the BIMCO Impact Levels [21] were selected as a confident measure for cyber incidents in the maritime sector, as they are currently used and validated in practice. Our game scenarios were constructed to carefully align to the three BIMCO impact levels, shown in Tabe 4.

Table 4: BIMCO Impact Levels, along with a summary of definitions and practical results of a potential security breach.

Impact and definition	**In practice, a security breach results in:**
Low (Limited adverse effect) - Loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on company and ship, organisational assets, or individuals.	• Degradation in ship operation to an extent or duration the organisation can perform its primary functions, but effectiveness is noticeably reduced. • Minor damage to organisational assets. • Minor financial loss. • Minor harm to individuals.
Moderate (Substantial adverse effect) - Loss of confidentiality, integrity, or availability could be expected to have a substantial adverse effect on company, ship, assets or individuals.	• Significant degradation in ship operation to an extent and duration the organisation can perform its primary functions, but effectiveness is significantly reduced. • Significant damage to organisational assets. • Significant financial loss. • Significant harm to individuals that does not involve loss of life or life-threatening injuries.
High (Severe adverse effect) - Loss of confidentiality, integrity, or availability could be expected to have a catastrophic adverse effect on company and ship operations, assets, environment or individuals.	• Severe degradation in or loss of ship operation to an extent and duration that the organisation cannot perform at least one primary function. • Major damage to environment or assets. • Major financial loss. • Severe harm to individuals involving loss of life or life-threatening injuries.

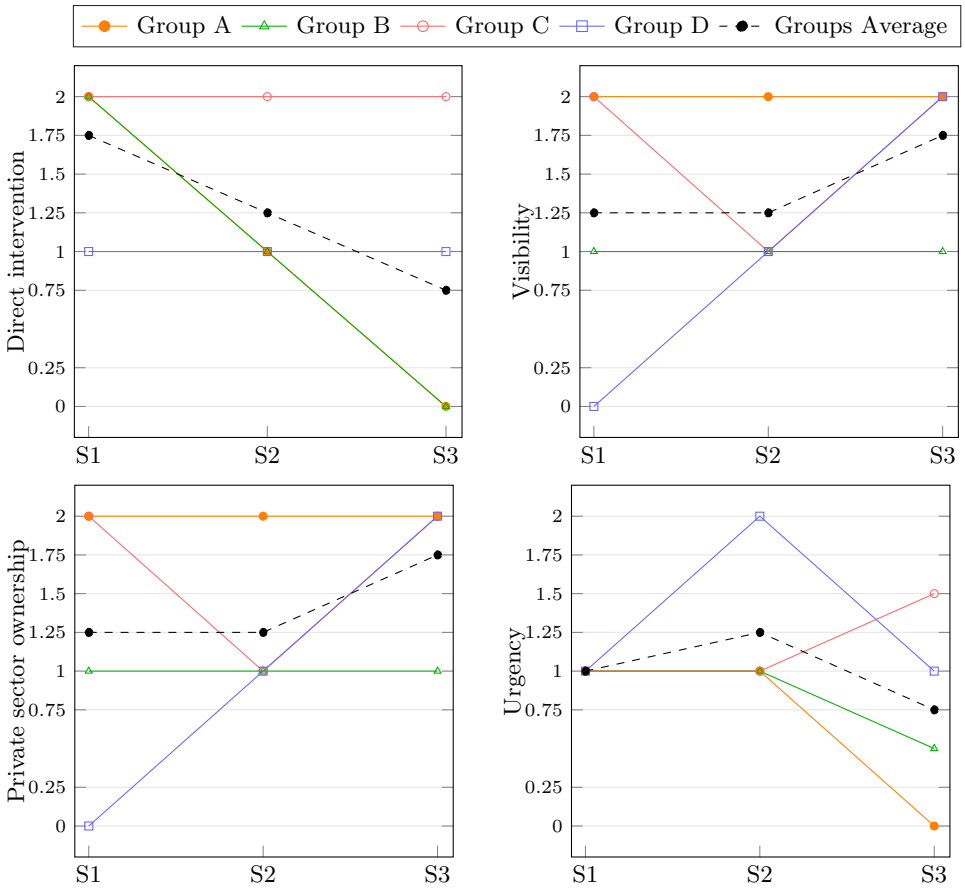
Source: BIMCO [21]

4.3 Incident response

In response to the second research question, which asks if work experience and cybersecurity expertise affect cyber incident response, participants rated four response characteristics for each of the three scenarios. Figure 4 shows

participant response to the changing impact levels. The trends suggest: The higher the impact of the incident, the response is less urgent, comes more from the private sector, is more visible and less direct.

Fig. 4: Group assessment of scenarios (S1, S2, S3) and incident response ranking.



5 Discussion

5.1 Understanding and assessing the participant group

In this participant group, there was great diversity in participant response to each response ranking. Figure 4 shows the participant group as a whole did not agree on a uniform response. As shown in Figure 2 and Figure 3, the sample had significant public/military sector experience (89 percent had five or more

years), but exhibited varied levels of private sector experience and cybersecurity expertise. Given this information, we may infer that significant public/military sector experience is a factor governing their response. This provides a lens through which the group results are interpreted.

We can confidently say that work experience, more specifically significant public/military sector experience, may affect cyber incident response. Indeed, previous work stresses the importance of *local memory* in how people make sense of cyber threats or incidents [24]. For this reason, we might expect the results to be framed by a pro-military bias, and a tendency to favor government-led response as opposed to private-sector led response.

Effective assessment of cyber risk perception of experts is done by calibrating risk, according to relevant guidelines, in a group setting. In this sense, we assume the participants, not the researchers, are the experts in the the room. Rather than measuring their results against an external benchmark, the group response as a whole is used to validate response. The value of this measurement increases with the number of participants who take part in the exercise- leading to greater calibration. Therefore, the results in this study can be strengthened with further iterations of the game. While this represents a limitation to this study, it is also a clear direction for future research.

5.2 Comparison of the group results

This section focuses on the trend lines for group average in Figure 4, which suggest: The higher the impact of the incident, the response is less urgent, comes more from the private sector, is more visible and less direct. Accounting for expert level work experience in the military/public sector, we may interpret the results of this study to understand tendencies of the participants group and infer about cyber incident response behaviors of NATO military officers and equivalent civilians.

First, group urgency of response decreases along with the impact of a cyber incident. This may reflect the idea that while small-scale cyber-attacks may be the work of criminals, larger-scale attacks are often the work of state actors, who are a more likely adversaries due to increased resources to support a complex attack and a long-term outlook. In this sense, "Law enforcement and military authorities seeking to check malicious cyber activity face another fundamental challenge: the 'attribution problem' of identifying the author of a cyber attack or cyber exploitation" [25]. While there may be pressure to name an adversary, the consequences of naming the wrong one early on often outweigh the cost of delaying response while information is gathered and verified. Indeed, the main hurdle is verification, which is difficult in the cyber realm due to attribution [25].

Second, as incident impact increased, group response favored more heavily the private sector, as opposed to the government, although the response did include a combination of both. This is interesting finding, as we estimated there would be a tendency to favor government-led response because in many countries military is closely aligned to state. Further, the 2019 Global Cyber Risk Perception Survey reports a "strong appetite for government leadership

and support" to help combat cyber threats [7]. However, the opposite is observed: as impact increased, group response favored the private sector.

One explanation is that as a cyber incident escalates, the government becomes reluctant to claim a mandate to oversee network security. However, it is often the case that the private sector is not inclined to accept responsibility or liability for national cyber security. This tendency is noted in previous work [26] concerning the challenges of public-private-partnerships. Another factor at play is that "The private sector has their hands deep in cyberspace in a way very difficult for the government to match" [27]. In other words, wide expansion of IT products and services makes it difficult for the government to keep up with the private sector, thus they rely on it. Consider that nearly 90 percent of US critical infrastructure is in private hands [28]. It is plausible this participant group, who comprise largely of military cybersecurity experts, are aware of this fact and thus rely on the private sector.

Third, group visibility of response increased along with the impact of the incident. This may have to do with a the fact that, while smaller incidents are easier to keep hidden or covert, large-scale cyber attacks are difficult to hide. Therefore, visibility reflects a greater need for assurance to those affected by and aware of the incident, for instance the public or the international community.

Finally, as incident impact increased, group response was less direct. This may be because as the impact of a cyber incident increases, so does its scale and complexity– to require a collective, and often multi-faceted response, especially in the context of NATO. This is evidenced in the previous example of "Cozy Bear" targeting Covid-19 vaccine researchers [1], whereas NATO was the first body to indirectly articulate information collected by various allies, including institution belonging to the Canadian, UK, and US governments.

This discussion provides insights into groups with significant public/military sector experience (more than five years). It may also, in this specific case, be used to explore tendencies which characterise the security culture of NATO and an emerging common risk perception.

5.3 Implications for practice

This study outlines key implications for NATO cybersecurity risk management in maritime cybersecurity, and for like organizations. First, it presents a cybersecurity decision-making game. This provides a way for decision-makers to grow familiar with acting amidst uncertainty, which is assumed to be an over-arching factor in cyber incident response. Further, "The simulation environment provides a context in which can implement various strategies in any number of repetitions without fear of real consequences" [6].

Second, this study sheds insights on an major aspect of complexity in managing cybersecurity in the maritime domain: cyber risk perception. This includes how to measure the risk perceptions of an expert group. We know that risk perception, though complex, is key to effective cyber incident response [19] and that incident response can be improved through iterative learning [6].

Hence, there is a need for further cybersecurity training tools within the NATO community, to reinforce proportionate response to cyber incidents. NATO has already made efforts to strengthen cybersecurity, evidenced in the over 200 training courses conducted at the COE-DAT center. They have also taken pains to manage cyber risk in maritime security, which include the NMIOTC center.

Despite these efforts, current training does not achieve shared situational awareness on cyber threats across NATO partners [4]. NATO can benefit from the findings of this study by incorporating cybersecurity decision-making game environments in their training, to challenge decision-makers and their risk perceptions, ultimately strengthening a shared security culture.

Our cyber game approach demonstrates that cyber risk perception is a key aspect of proactive decision-making, and can be not only measured, but improved significantly through iterative learning. Such games can be used to develop training materials that better address the educational needs of NATO military officers and civilian equivalents.

6 Conclusion

Using our cybersecurity decision-making game, we focus on understanding how cybersecurity experts perceive cyber risk and respond to incidents to strengthen decision-making and preparedness. In general, there are two main findings that contribute to maritime cyber risk perception and response:

- Effective assessment of cyber risk perception of experts can be done by calibrating risk, according to relevant guidelines, in a group setting.

- As incident impact rises, groups with strong public/military sector experience and mixed cybersecurity expertise respond in favor of private sector responsibility and visibility, but not in favor urgency or directness.

According to the Atlantic Council, "NATO remains the world's most successful alliance because it has been able to adapt to new challenges" [12]. In this respect, NATO must continue to address a shifting cyber threat landscape, and they acknowledged exactly this in a June 2020 statement [1]: "NATO will continue to adapt to the evolving cyber threat landscape."

This exercise is a tool for NATO partners to prepare and plan cyberspace operations in the maritime environment. Effective risk perception and response are key to mitigate cyber incidents. By refining technological skills and decision-making, participants can address a key disconnect in crisis response. This exercise, trialled successfully in small setting, offers insights into how games can build capacity and echoes the need for joint response.

References

1. North Atlantic Treaty Organization. Statement by the north atlantic council concerning malicious cyber activities. 2020.
2. National Cyber Security Centre. Uk and allies expose russian attacks on coronavirus vaccine development. 2020.
3. North Atlantic Treaty Organization. Active engagement, modern defence: Strategic concept for the defence and security of the members of the north atlantic treaty organization, 2010.
4. Bruno Lété and Piret Pernik. *EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*. German Marshall Fund of the United States, 2017.
5. Sally McNamara. NATO summit 2010: Time to turn words into action. *Backgrounder". Published by The Heritage Foundation*, (2498):2, 2010.
6. Mohammad S. Jalali, Michael Siegel, and Stuart Madnick. Decision-making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment. *The Journal of Strategic Information Systems*, 28(1):66–82, 2019.
7. Marsh LLC and Microsoft. 2019 global cyber risk perception survey. Technical report, Marsh LLC and Microsoft, 2019.
8. NCSC. Cyber Security Toolkit for Boards 2019. Technical report. available from `https://www.ncsc.gov.uk/collection/board-toolkit`.
9. Palmer, D. A. R. New operational horizons: Nato and maritime security, 2007.
10. Council, NATO North Atlantic. Riga Summit Declaration, November 29, 2006.
11. Caton, Jeffrey L. Nato cyberspace capability: A strategic and operational evolution. Technical report, Army War College-Strategic Studies Institute Carlisle United States, 2016.
12. Hans Binnendijk and Timo S. Koster. Nato needs a new core task. *Defense News*, 2020.
13. G. Tsogkas. Nmiotc commandants editorial. *NMIOTC MIO Journal, 14th Issue*, 2017.
14. Atif Hussain, Siraj Shaikh, Alex Chung, Sneha Dawda, and Madeline Carr. *An Evidence Quality Assessment Model for Cybersecurity Policymaking*, volume (542), pages (23–38). Springer, Cham, 2018.
15. Framework for improving critical infrastructure cybersecurity. Technical report, National Institute of Standards and Technology, 2018.
16. Douglas W Hubbard. *The failure of risk management: Why it's broken and how to fix it*. John Wiley & Sons, 2020.
17. George O Rogers. Residential proximity, perceived and acceptable risk. In *Low-Probability High-Consequence Risk Analysis*, pages 507–520. Springer, 1984.
18. Zur Shapira. *Risk taking: A managerial perspective*. Russell Sage Foundation, 1995.
19. Michael J Williams. *NATO, security and risk management: from Kosovo to Khandahar*. Routledge, 2008.
20. Atif Hussain, Kristen Kuhn, and Siraj Ahmed Shaikh. Games for cybersecurity decision-making. In *HCI-Games: 2nd International Conference on HCI in Games*, pages In–press. Springer, 2020.
21. BIMCO, CLIA, ICS, Intercargo, Intermanager, Intertanko, IUMI, OCIMF and World Shipping Council. The guidelines on cyber security onboard ships- version 3. 2018.

22. Eric Stern. *Designing crisis management training and exercises for strategic leaders: A Swedish and United States Collaborative project.* National Defense College, 2014.
23. Atlantic Council. Cyber 9/12, 2020. available from `https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/cyber-912/`.
24. Gordon Walker, Peter Simmons, Brian Wynne, and Alan Irwin. Public perception of risks associated with major accident hazards. *HSE Contract Research Report*, 1998.
25. Jack Goldsmith. How cyber changes the laws of war. *European Journal of International Law*, 24(1):129–138, 2013.
26. Madeline Carr. Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1):43–62, 2016.
27. Jason Healey. Who's in control: Balance in cyber's public-private sector partnerships. *Geo. J. Int'l Aff.*, 18:120, 2017.
28. Dave Weinstein. America's cyber blind spot. *Geo. J. Int'l Aff.*, 2019.