On the Use and Strategic Implications of Cyber Ranges in Military Contexts: A Dual Typology

Andrew C Dwyer[1], Kathrin Moog[2], Jantje Silomon[2] and Mischa Hansel[2]
[1] Information Security Group, Royal Holloway, University of London, Egham, UK.
[2] Institute for Peace Research and Security Policy at the University of Hamburg, Germany.

andrew.dwyer@rhul.ac.uk
moog@ifsh.de
silomon@ifsh.de
hansel@ifsh.de

Abstract: The use of simulated environments in cybersecurity – cyber ranges (CRs) – has become a popular method and tool to support training and education, assess system vulnerabilities, as well as to test and probe computer networks. Yet, CRs can be adopted to improve and enhance adversarial skill sets, tools, and operations that are attractive for military applications. This paper develops a strategic typology on how CRs have been used and adopted in military contexts (CRiMCs), where states have turned to CRs as one method to build cyber capacity, address proportionality and responsibility of cyber operations, as well as offer training and education. We identify CRiMCs that offer two strategic purposes: 1) reserved for sovereign use and capability development and 2) those intended to support cyber capacity building through domestic resilience and collaborative inter-state exercises. We thus ask, why do states establish sovereign cyber ranges 'on top' of being involved in collaborative ones? Why and how do they differ? To answer such questions, this paper delves into both the crucial technical components that support each CRiMC type and their implications by offering exemplars from five states (Lithuania, Norway, Slovenia, the Netherlands, and the USA). The paper concludes with some preliminary thoughts on future research avenues on CRiMCs and their implications for the use and governance of state cyber capabilities.

Key Words: Cyber Ranges; Cyber Operations; Cyber Capacity Building; Typology; Cyber Strategy

1. Introduction

Establishing environments for testing and training are core to military thinking and development. Within cybersecurity, as computational networks have spread across society, this has stimulated a burgeoning industry offering training and assessing system vulnerabilities through the provision of virtual environments – cyber ranges (CRs). These have become popular in commercial and research applications, from testing cybersecurity response readiness to education and training, as much as they have had a sustained history and development in their use by militaries (Davis and Magrath, 2013). However, there has been relatively little examination of the *strategic* use of CRs in military contexts (CRiMCs) beyond an analysis of their technology and little on how they have been used by states to enhance their cyber capabilities, operations, and campaigns.

The building of cyber capabilities and their use to engage in inter-state competition has become increasingly commonplace, with a growing diffusion of military cyber forces across the world dedicated to such activity (Blessing, 2021; Smeets, 2022a). As cyber capabilities have stretched beyond 'cyber powers' such as the United States, Russia, and China, a greater number of states are seeking to exploit computational networks for both pre-emptive defence and to pursue various effects against adversaries. Such activity has frequently occurred beyond the conventional bounds of war, in what Kello (2017) identifies as a condition of 'unpeace'. Amid a strategic posture of persistent engagement by states through continuous operations and campaigns rather than standalone vulnerabilities or 'weapons', as argued in contemporary US doctrine (Fischerkeller et al., 2022), an increased operational tempo requiring regular assessments and investment to ensure operational effectiveness is required. The proliferation and use of state cyber capabilities has likewise been accompanied by a greater attention to the applicability of international law in cyberspace and commitments to non-binding rules on responsible behaviour (Painter, 2021). Thus, there is an ethical as well as normative commitment to ensure cyber operations are precise, proportionate, and responsible in their use.

We examine the application of CRs in this broader military context, identifying how they could be strategically used in a changing operational landscape. Although CRiMCs have existed since at least the early 2010s, such as the US National Cyber Range (US NCR) initiated by DARPA (Davis and Magrath, 2013; Rosenstein and Corvese, 2012). This does not only apply to international military cooperation (Miller, 2022), but also their domestic economic opportunities as well as sovereign capabilities as part of NATO's Cyber Range developed through Foundation CR14 in Estonia (2022). This paper then provides two key contributions. First, it develops a strategic typology of CR application to understand their integration and use by states in military contexts. These are split

into two categories of CRiMCs, centred on pursuing sovereign objectives and capabilities on the one hand, and demonstrating and enabling cyber capability building measures – both domestically and internationally – on the other. Second, it explores this typology to understand the strategic implications of CRiMCs for states. The paper then proceeds by: 1) offering a background on CRs and their use in military contexts; 2) setting out our empirical analysis and giving a brief overview to five states and developing a typology of CRiMCs into those for sovereign use and capacity building; before, 3) discussing the strategic implication of CRiMCs for states and their future applications.

2. Cyber Range Architecture and Use

CRs have become popular across industry and strategically for state actors, for example within China (Cary, 2022). Defined as "interactive, simulated platforms and representations of networks, systems, tools, and applications" (National Initiative for Cybersecurity Education, 2020, p. 3), they can be used for a variety of purposes, but primarily for training and skills development (Turčaník, 2020). This has led to a range of typologies on their architecture and use. For instance, academic literature makes a distinction between CRs and testbeds (Davis and Magrath, 2013; Ukwandu et al., 2020), with the latter often referring to the testing of operational technologies (OT). Much work has sought to likewise create different categories of use to apply to different types of groups and their technical architecture (Karjalainen and Kokkonen, 2020; Urias et al., 2018), as well as their military use (Debatty and Mees, 2019). Päijänen et al. (2021), for instance, identify both 'government' and 'military cyber defence capabilities' as target groups for CRs, and identify international exercises by states as one implementation. However, apart from their application to capacity building, their utility for the deployment of cyber operations and capabilities by states is underexplored. We therefore bridge an analysis of strategic use by states for their cyber capabilities and their technical manifestation, as we explore in our typology below.

CRs can, to some extent, be seen as a compromise: a large-scale and flexible environment allowing for complex scenarios that are predominantly virtualised (but can include emulation and hardware integration). CYBERWISER (2020), for example, uses a three-tiered categorisation based on functional capabilities:

- a simple, pre-defined, network-accessible but limited environment;
- a locally accessible infrastructure into which malware cannot be introduced; and,
- a large, complex, locally accessible infrastructure where all equipment and devices are provided by the cyber range vendor/operator, and malware may be safely run.

Furthermore, CRs cover a vast variety of systems and thus technical arrangements – a range focused on an industrial control system (ICS) will have limited use cases compared to generic 'off-the-shelf' set-ups more common in commercial and research applications. Yet, certain basic elements will be recognisable, including the three key architectural components: underlying infrastructure, orchestration, and range capabilities (ECSO, 2020; Ukwandu et al., 2020).

2.1 Three Architectural Components

Historically, CRs underlying *infrastructure* tended to rest entirely on dedicated hardware, such as utilising large, localised server racks, with systems built 'directly on top' of physical infrastructure. While such dedicated systems can remain important for some CRiMCs – both for enhanced security and enabling high fidelity capacities, particularly when simulating highly specialised or proprietary software and hardware, they continue to be expensive to construct and often lack flexibility. Coupled with advances in virtualisation and cloud technologies, CRs can be adapted to be economically efficient and iteratively updateable, which have gained widespread acceptance, particularly for commercial and research focussed CRs.

Orchestration combines two main aspects, the CR's environmental set-up and its management. The former includes, for example, automated configuration and coordination that becomes important when CRs are required to be reiterated frequently. Whereas the latter refers to elements such as attack scheduling and event injection to enable realistic scenarios.

Range capabilities are split into two main parts. The first is a type of learning management system used by the white team and can include scoring, guiding, and/or decisions. It can also be used to inform a green team, whose purpose is to maintain and repair/fix issues. The second is the target system, including their underlying

infrastructure (e.g., endpoints, servers, storage, applications, and networks), security operations (e.g., SIEMs and IDS), and the 'outside' (e.g., wider domains, proxies, DNS). While these will be present in both CRs and CRiMCs, and blue/red teaming might be conducted, the detail and complexity will vary. Similarly, so will the system response, which could be scripted, automated, live, or a combination thereof.

2.2 Adversarial Uses

Many scenarios might test how well an organisation responds against adversary behaviours and malware, such as well-known examples like WannaCry or Emotet. Or in the case of more OT-centred ranges, malware such as Triton, first discovered at a Saudi Arabian petrochemical plant in 2017, could be used. However, they can be deployed for adversarial uses too, which is critical for some CRiMCs applications. They may be used to build simulated environments of adversaries which states can test their capabilities against. A highly advanced and now infamous example – which may be described as a CRiMC – are those created for the Olympic Games broader suite of operations, commonly abridged to the Stuxnet malware (Zetter, 2014). In preparation for a series of interconnected operations against the Natanz nuclear enrichment facility in Iran by the USA, Israel, and other states, extensive CRiMCs were constructed. This hardware-software cyber testing was at least partially conducted at the Dimona nuclear plant in southern Israel as well as in the US at Oak Ridge (ibid). Thus, CRiMCs may not be singular or concentrated in one place, but constructed of various components, with shared data and facilities, or even testing for different components. Although Olympic Games and Stuxnet may represent the one – and only – publicly known example of the extensive fine-tuning of cyber capabilities through testing, the result was a stealthy and, importantly, highly-targeted, and discriminate operation that did not cause significant impact outside of its intended target. Despite its wide-spread propagation, it was designed to lay dormant before deletion, increasing its covert appeal and reducing the chances of its detection and consequent unintended impacts.

Despite the reported in-depth capabilities on display for Stuxnet, most states and cannot financially sustain or deploy the required skills for such testing alone. They may also have military cyber forces that can only engage in cases of armed conflict, i.e., only 'above' the threshold. Therefore, many states that may wish to test their capabilities are reliant on either international cooperation or on private enterprise, primarily from the defence and aerospace industry, to develop, maintain, and implement CRiMCs. These can fulfil a training role as much as other non-military and non-offensive capabilities testing. In most cases, generic set-ups for adversarial purposes are unlikely to be used unless states wish to test out how susceptible a common environment may be. Detailed target knowledge – sustained by significant intelligence collection – will not only improve operational effectiveness but could also help prevent collateral damage or unintended consequences, a requirement for a 'responsible' actor. Yet detailed knowledge of the target's environment, particularly its technical components, requires insights that may only be acquired by already having presence inside an adversary's environment. Knowing that one specific PLC is used without its detailed integration and implementation is unlikely to be sufficient. Instead, various component and subcomponent vendors might need to be known, or details such as the frequency band of motor spin systems, as Stuxnet demonstrated.

3. CRiMC Typology

CRs thus exhibit a wide range of applications, uses, and varying technological requirements, leading to greatly differing definitions and their application in military contexts. Using the categories laid out by CYBERWISER (2020), for example, only the third– a large, complex, and locally accessible infrastructure - could be considered relevant. However, underlying *infrastructure* options would have to include cloud-based components, at least in some cases. This aspect, as well as the range capabilities, are likely to diverge the most between CRs and CRiMCs, though again dependent on their intended use. In this section, we develop a typology of CRiMCs from research of public documentation: first, those reserved for sovereign capabilities by states and second those used to enable domestic and international cyber capacity building.

3.1 Methodology

To identify CRiMCs, we analysed public documentation primarily available in English for forty-six states in the European region, Canada, and the USA up to August 2022. This included the analysis of national cyber strategies, official announcements, as well as public news sources to understand the diffusion, and use, of CRiMCs by states.

Our preliminary analysis then identified thirty-six states using CRiMCs, demonstrating their often-complex arrangements. For example, Spain's Joint Cyber-Defence Command used the Minsait Cyber Range system by the private enterprise Indra to conduct both capacity building, information sharing, as much as to "conduct and execute military operations in cyberspace" (Indra, 2019). The quote is however demonstrative of the openness to interpretation of such materials – and does not signify, for example, that offensive cyber operations are tested on this CRiMC.

The publicly available information on CRiMCs is scarce, resulting in several limitations. When there is information, it is often brief and lacks details to appropriately assess how a CRiMC is used by a particular state. In our research, there is little, if any, technical detail on CRiMCs, their funding or intended use. With a few exceptions, such as the US NCR with more regular updates, many sources are vague, difficult to corroborate, and timely information is not routinely maintained. This is also compounded by the limitation of reviewing predominantly English-language documentation, which is likely to restrict insight into documentation produced by various states.

3.2 CRiMC Analysis

Table 1 presents our initial analysis of data from forty-six states as of August 2022, demonstrating a wide variety of states that engage in the usage of CRiMCs, with many owning CRs to use for capacity building, particularly domestically. However, far fewer have publicly declared CRiMCs for sovereign use that are unambiguous. The analysis of public documentation resulted in either a confirmation of existence or use ('✓'), sufficient to deem that it does not exist or is used ('✕'), or for situations of ambiguity or lack of information ('**?**').

Therefore, the data presented offers only an indicative analysis of how states are primarily organising their CR capabilities, where their sovereign use and ownership emerged through the data analysis. This typology then emerged during the analysis of states' strategic use of CRs between sovereign and capacity building capabilities that we define below as:

1. Sovereign CRiMCs: CRs for the exclusive development of sovereign cyber capabilities; primarily for honing active cyber operations and campaigns against adversaries but may expose vulnerabilities that can be used for improving a state's domestic cyber security.
2. Capacity Building CRiMCs: CRs to enhance defensive capability, complement and federate CRs, as well as share information and training both domestically and between states.

Below we present five cases in greater detail to demonstrate the different uses and ownership of CRiMCs before detailing how they technically and strategically differ in 3.3. Each case has a short description of its regional position and how it uses CRiMCs. This is not intended to be a systemic representation of CRiMCs but rather a descriptive interpretation of the range of configurations for their use and ownership. This means that we seek to include states that engage in capabilities across both sovereign and capacity building use, engage internationally and domestically, and how different models of ownership ranging from being exclusively in miliary settings to more collaborative set-ups.

3.2.1 Lithuania

A Baltic state using a cyber capacity CRiMC based within national defence including international cooperation.

In 2022, *Virtualus Kibernetinis Poligonas* was deployed as a new CRiMC (Lithuanian Ministry of National Defence, 2022), with an investment of €800,000. It has a range of uses, enabling the "simulation of cyber-attacks of different levels in a safe closed environment" (ibid). This includes CTFs as well as real-time team exercises, accessed remotely. It is intended to be used by staff from defence, cybersecurity actors in Lithuania, as well as foreign partners. The CRiMC is run by the National Cyber Security Centre under the Ministry of National Defence.

3.2.2 Norway

A Nordic state using a cyber capacity CRiMC in an academic setting, with defence funding, as well as with international cooperation.

The Norwegian Cyber Range is based within the Norwegian University of Science and Technology (NTNU) to enable cooperation between government, business, and academia launched in 2018 (NTNU, 2022), funded with ~€7 million. The CRiMC has both remote and physical access (from 2022) with support from the Norwegian

armed forces. It is also part of an "Open Cyber Range" with Estonia intended for cybersecurity training in the private and education sectors (Norwegian Ministries, 2019).

Table 1: An overview of CRiMC use and ownership according to our outlined typology.

State	CRiMC use in public documentation	CRiMC owned for sovereign use	CRiMC owned for cyber capacity building
Albania	✓	×	×
Armenia	?	?	?
Austria	✓	×	✓
Azerbaijan	?	?	?
Belarus	?	?	?
Belgium	✓	×	✓
Bosnia and Herzegovina	×	×	×
Bulgaria	✓	×	✓
Canada	✓	×	✓
Croatia	✓	×	×
Cyprus	×	×	×
Czechia	✓	×	✓
Denmark	✓	?	?
Estonia	✓	✓	✓
Finland	✓	×	✓
France	✓	×	✓
Georgia	✓	×	×
Germany	✓	×	✓
Greece	✓	×	✓
Hungary	✓	×	✓
Iceland	?	×	×
Ireland	✓	×	✓
Italy	✓	?	✓
Kosovo	×	×	×
Latvia	✓	×	✓
Lithuania	✓	×	✓
Luxembourg	✓	×	✓
Malta	✓	×	✓
Moldova	?	?	?
Montenegro	?	?	?
The Netherlands	✓	✓	✓
North Macedonia	?	?	?
Norway	✓	×	✓
Poland	✓	×	✓

Portugal	✓	×	✓
Romania	✓	×	✓
Russia	✓	?	✓
Serbia	✓	×	✓
Slovakia	✓	×	✓
Slovenia	✓	×	✓
Spain	✓	?	✓
Sweden	✓	×	✓
Switzerland	✓	×	✓
Turkey	?	?	?
Ukraine	✓	×	✓
United Kingdom	✓	?	✓
USA	✓	✓	✓

3.2.3 Slovenia

A central European state with a cyber capacity CRiMC supported by another state.

Slovenia's CRiMC is supported by €12.7 million from the United States' European Command to incorporate a range of different activities and actors from academia, private research, and civil society (U.S. Embassy in Slovenia, 2020). This is being combined in the Slovenian Ministry of Defence with its Security Operations Centre (Slovenian Republic, 2022). There is no detail on its technical set-up.

3.2.4 The Netherlands

A western European state with a CRiMC for both sovereign and cyber capacity capabilities.

Limited information about a sovereign cyber range built for Defence Cyber Command (DCC) in 2016 by private defence contractor Thales was identified. It is used for training and development as well as "to acquire and test new cyber-defence techniques at an early stage." As the then-Commander, Hans Folmer, said, "[i]t is a facility at which many forms of cyber operations can be simulated" (Thales, 2016). There is little information post-2016 about subsequent activities beyond the initial press release, which stated it would only last for 3 years.

3.2.5 United States

A North American state with multiple CRiMCs for both sovereign and cyber capacity capabilities with international cooperation.

The US National Cyber Range (NCR) is one of several CRiMCs, with the NCR initiated by DARPA to build an Internet-like environment, since at least 2008 (DARPA, No Date), with a range of different technical components that enable both classified and unclassified use by a variety of actors. In 2021, the U.S. Army awarded part of a $2.4bn contract for a range complex to BAE Systems (2021). Similarly, there has been clear offensive capability on the range, as much as it is used for multi-country exercises, such as annual USCYBERCOM exercises, with physical and remote, cloud-based access. As a recent Department of Defense press release noted, "the NCR enables DOD to conduct virtual, combined and joint cyberspace training, exercises, mission rehearsals, experiments and certifications… enabl[ing] a high degree of collaboration, development of U.S. and allied cyber tactics, techniques and procedures for defensive cyber missions" (U.S. Cyber Command, 2021). This is only a limited snapshot of the US NCR, which has developed and evolved over time, with a great deal of detail on its composition and activities.

3.3 Sovereign and Capability Building Uses

3.3.1 Sovereign CRiMCs

The identification of sovereign uses of CRiMCs is difficult but is ambiguously implied across various documentation and most explicitly in the case of the Thales-built cyber range in the Netherlands. Likewise, sovereign use is enabled through the segregation between classified and unclassified networks in the US NCR. Such sovereign uses will have different technical features compared to those for capacity building due to their alternative strategic nature. They are more likely to:

- Require emulation or high-fidelity simulations of environments in which to test capabilities. This means they resemble arrangements closer to testbeds with cyber-physical capacities to identify precise analysis for cyber operations to enhance responsibility and promote covertness.
- Embed hardware when wishing to robustly test against specific assets and adversaries.
- Require flexible and effective environments and scenario planning, with integration of active intelligence for unique implementations.
- Have greater attention to authentication, vetting of personnel, and segregation of networks (to limit attacks against CRiMCs themselves).

This is not an exhaustive list and the technological requirements for sovereign CRiMCs will require alternative arrangements, which, in turn, are discussed less in the public domain. Hence, it is difficult to appropriately test empirically these claims from public documentation.

3.3.2 Capacity Building CRiMCs

Capacity building – particularly through training and education – is a key feature of most CRs, whether that is in corporations, universities, or in enhancing the cybersecurity of state bureaucracies. This is replicated in CRiMCs, where it is possible to sub-divide their use according to:

1. *Domestic Capacity Building*: This is seen in almost all CRiMCs, where their dual – and even multiple – uses extend in complex ways. For example, with the US NCR, the invitation of improving domestic civilian cybersecurity is deemed crucial. This is even more so in the case of the Norwegian cyber range, which is primarily focused on such capacity building albeit supported by the armed services.
2. *Inter-State Capacity Building*: This is where states are sharing CR resources – such as through wargaming – to enhance another state's (and potentially their own) cybersecurity. Lithuania seeks to invite foreign stakeholders into their CRiMC, whilst the US explicitly uses its NCR to build allied capacities for security. In the most extreme case, we could see the US's funding of Slovenia's CRiMC as evidence of this form of capacity building indirectly.

In contrast to sovereign CRiMCs, Capacity Building CRiMCs are about demonstrating shared commitments to improve cybersecurity (and in the process of wargames scenarios, *abstracted* counter-adversary capabilities). Such capacity-building CRiMCs share similar technological attributes – with focuses on CTFs, integration of third-party actors often via cloud technologies, can be similar to those built by commercial providers, and have environments that are more generically modifiable with known vectors. Unlike most CTFs, however, these CRiMCs not only have dedicated infrastructure and resources, but are also more formalised in state or state-sponsored institutions.

Capacity building can also include the explicit sharing of training, information on best practice and the pooling of cyber ranges to extend capacity. One example of this is through the EU's Cyber Federations project, launched in 2017 and renewed in 2021 (European Council, 2021), which seeks to interconnect several EU cyber ranges into a larger cluster or CRiMCs developed at NATO. This is not too dissimilar from the US NCR, which combines several different technical components to build a larger cyber range with shared facilities that can be remotely accessed.

3.4 Making a Distinction Between CRiMCs

In the technical distinction of CRiMCs between sovereign and capacity building purposes, we do not assert that they must be mutually exclusive. CR architecture may permit both sovereign and capacity building (for example, as the US NCR does). Rather, attention must be paid to the CR orchestration and range capabilities in context. There is strong technological and strategic reasoning – to maintain secrecy, enable covert activity, and reducing the attack surface of CRiMCs – for separating out sovereign and capacity building capabilities. Assuring and

protecting CRs when engaging active sovereign capabilities – such as cyber operations against adversaries – requires greater investment. It is unlikely that most states would be able to have the expertise and capacity to configure both uses on the same CR, even when federated, apart from a very limited number of actors, such as in the US. There is therefore a close connection between the strategic ambitions for the use of CRs and their technical manifestation, as much as the latter then shapes the strategic possibility for most states due to the cost and expertise required to build and maintain sovereign CRiMCs. This is likely why there are many states engaging in CRiMCs, particularly with capacity building both domestically and internationally. This is because they frequently replicate 'off-the-shelf' commercial products, with preconfigured information on such CRs being transferable, as much as they offer more advantageous security and economic benefits for states. However, the public documentation on sovereign use is likely reflective of the strategic ambitions of states to engage in sustained cyber operations – such as the United States and the Netherlands. Other states may not wish to publicly declare CRs for sovereign capabilities to avoid declaring a more active strategic posture, thus this analysis underreports the extent of their use by states.

4. Strategic Implications

Based on the CRiMCs typology and analysis outlined above, there are multiple strategic implications for states and the practice of cybersecurity. This section offers three pertinent, but not exhaustive, set of issues: first on the maintenance of sovereign capabilities, the development of responsible behaviour and second on what the use of CRiMCs means for state signalling. More detailed exploration of deterrence aspects and potential escalation risks is not within the scope of this paper but subject of further research.

4.1 Maintaining Sovereign Capabilities

As recently pointed out by Smeets (2022b), states are reluctant to share cyber capabilities with allies and partners, partly due to the transitory nature of these capacities. There is an increased risk of detection that could 'burn' an information advantage, for instance with backdoors or zero-days. Such thinking can be applied to CRiMCs, as sharing technical details about the CR's architecture, orchestration or capabilities may expose details on a state's intelligence collection and integration that could be maliciously used to reverse engineer the CR or introduce false information and data. Indeed, a CRiMC for sovereign capabilities may assist in greater precision, proportionality, and operational tempo that states may see as increasing the effectiveness of cyber operations. Instead of the risk of transferring sovereign capabilities and losing a potential competitive advantage, states therefore engage in less risky capacity-building measures including cyber exercises, intelligence sharing, or funding CRiMCs as the US has in Slovenia even if they have a sovereign CRiMC. This supports the assertion that states wish to maintain exclusive technical competency at some level, even as joint exercises, such as NATO's Locked Shields, are on the rise.

4.2 Responsible Behaviour

For years, cyber diplomats have discussed principles of due diligence and state responsibility in cyberspace. As part of the eleven non-binding norms adopted by various fora of the United Nations, states voluntarily agreed not to target critical national infrastructures nor target emergency computer response teams (United Nations, 2021). Beyond this, states have also noted that the targets of attacks must therefore not be indiscriminate and maintain proportionality. The use of CRiMCs, particularly those geared towards sovereign uses, could stimulate adherence to these norms through testing of both capabilities and increased training and education, especially for state militaries who only act during armed conflict and wish to maintain operational effectiveness. However, more empirical research is needed to assess whether CRiMCs are helpful in reducing collateral damage and in encouraging responsible and proportionate behaviour. There is also the question how to avoid capability gaps and operational friction between allies, particularly if only sovereign CRiMCs enable significant advancements in conducting discriminatory and proportional cyber operations.

4.3 Signalling

CRiMC's development and use could have important signalling effects. For example, they might partially substitute 'real weapons tests' by signalling advanced capabilities for training and operational planning. States sharing some access to CRiMCs of their allies could hope to benefit from an extended deterrence effect, such as

in the case of the US NCR. That said, some states do not have CRIMCs or do not advertise them, as seen in Table 1. Others barely acknowledge theirs, as for example in in the case of the Netherlands. Based on the signalling argument, the lack of a CRiMC or their explicit acknowledgement could perhaps be seen to undermine a state's cyber deterrence, however further research will be required to assess this. In general, we contend that certain cyber ranges, specifically those simulating specific target systems, are very unlikely to be revealed for signalling purposes, since doing so would dramatically reduce their operational value and come with a heightened risk of intelligence loss. Acknowledging the existence of cyber ranges that were used in preparation of past cyber operations could be a different matter though. However, states may refrain from this due to legal and political risks, i.e., the same reason why there is rarely self-attribution of specific cyber operations.

5. Conclusions

This paper has explored the role of states in cyber ranges for military contexts – CRiMCs. Through a preliminary analysis of forty-six states, and the use of five indicative cases of Lithuania, Norway, Slovenia, the Netherlands, and the USA, a strategic typology of their use by states was developed. They were divided into 1) sovereign CRiMCs for the development of sovereign cyber capabilities and 2) capacity building CRiMCs that enhance both domestic cybersecurity as well as foster inter-state use and information sharing. Through this, both the technical and strategic underpinnings for such a distinction were assessed. However, due to limited public documentation and ambiguous language, the paper does not claim to be able to assess the relative distribution of each type within the international system. Different methods of data collection, such as expert interviews, will be required to overcome the limitations of public documentation for technical detail as well as the strategic ambiguity that many states employ regarding cyber operations. Other questions relate to the strategic relevance of CRiMCs. Beyond improving the effectiveness and responsibility of cyber operations, they could play a role in signalling and thus have a deterring effect. Since the latter is dependent on a minimum degree of transparency, future studies could take a closer look into the differences of public communication about CRiMCs across states. Systemically applying CRiMCs in a capacity building manner could offer novel ways to share the burden and expense of CRs but could also entail risks, which will also be the focus of future research.

References

BAE Systems, 2021. BAE Systems selected for National Cyber Range Complex contract [WWW Document]. URL http://web.archive.org/web/20221029102424/https://www.baesystems.com/en/article/bae-systems-selected-for-national-cyber-range-complex-contract (accessed 10.29.22).

Blessing, J., 2021. The global spread of cyber forces, 2000–2018. Presented at the 2021 13th International Conference on Cyber Conflict (CyCon), IEEE, pp. 233–255.

Cary, D., 2022. Downrange: A Survey of China's Cyber Ranges (Issue Brief). Center for Security and Emerging Technology, Washington, D.C.

DARPA, No Date. The National Cyber Range: A National Testbed for Critical Security Research.

Davis, J., Magrath, S., 2013. A survey of cyber ranges and testbeds (No. DSTO-GD-0771). Cyber and Electronic Warfare Division, Defence Science and Technology Organisation, Department of Defence, Australian Government, Edinburgh, South Australia.

Debatty, T., Mees, W., 2019. Building a Cyber Range for training CyberDefense Situation Awareness, in: 2019 International Conference on Military Communications and Information Systems (ICMCIS). Presented at the 2019 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1–6. https://doi.org/10.1109/ICMCIS.2019.8842802

European Council, 2021. EU defence cooperation: Council launches the 4th wave of new PESCO projects [WWW Document]. URL http://web.archive.org/web/20221029124750/https://www.consilium.europa.eu/en/press/press-releases/2021/11/16/eu-defence-cooperation-council-launches-the-4th-wave-of-new-pesco-projects/ (accessed 10.29.22).

Fischerkeller, M.P., Goldman, E.O., Harknett, R.J., 2022. Cyber Persistence Theory: Redefining National Security in Cyberspace. Oxford University Press.

Foundation CR14, 2022. CR14 NATO Cyber Range [WWW Document]. URL http://web.archive.org/web/20221031160920/https://cr14.ee/ (accessed 10.31.21).

Indra, 2019. The Joint Cyber-Defence Command completes its training with Indra Cyber Range [WWW Document]. Indra. URL

http://web.archive.org/web/20221024113226/https://www.indracompany.com/sites/default/files/190717_pr_indra_cyber_range_-_mando_conjunto_ciberdefensa.docx.pdf (accessed 10.24.22).

Karjalainen, M., Kokkonen, T., 2020. Comprehensive Cyber Arena; The Next Generation Cyber Range, in: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Presented at the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 11–16. https://doi.org/10.1109/EuroSPW51379.2020.00011

Kello, L., 2017. The Virtual Weapon and International Order. Yale University Press, New Haven.

Lithuanian Ministry of National Defence, 2022. Cyber Range of the National Cyber Security Centre unveiled [WWW Document]. URL https://kam.lt/en/cyber-range-of-the-national-cyber-security-centre-unveiled/ (accessed 10.29.22).

Miller, M., 2022. NATO prepares for cyber war. Politico.

National Initiative for Cybersecurity Education, 2020. The Cyber Range: A Guide (Draft Guidance). NIST.

Norwegian Ministries, 2019. List of measures – National Cyber Security Strategy for Norway.

NTNU, 2022. Norwegian Cyber Range [WWW Document]. URL https://www.ntnu.no/ncr (accessed 10.29.22).

Päijänen, J., Saharinen, K., Salonen, J., Sipola, T., Vykopal, J., Kokkonen, T., 2021. Cyber Range: Preparing for Crisis or Something Just for Technical People? Presented at the ECCWS 2021 20th European Conference on Cyber Warfare and Security, Academic Conferences Inter Ltd, p. 322.

Painter, C., 2021. The United Nations' cyberstability processes: surprising progress but much left to do. J. Cyber Policy 6, 271–276. https://doi.org/10.1080/23738871.2021.2014920

Rosenstein, M., Corvese, F., 2012. A Secure Architecture for the Range-Level Command and Control System of a National Cyber Range Testbed, in: 5th Workshop on Cyber Security Experimentation and Test (CSET 12). USENIX Association, Bellevue, WA.

Slovenian Republic, 2022. Izvedbeni načrt za izpolnjevanje kriterijev in zavez Republike Slovenije za Stalno strukturno sodelovanje na področju varnosti in obrambe Evropske unije (PESCO).

Smeets, M., 2022a. No Shortcuts: Why States Struggle to Develop a Military Cyber-Force. C Hurst & Co Publishers Ltd, London.

Smeets, M., 2022b. Why NATO Countries Don't Share Cyber Weapons. Natl. Interest. URL http://web.archive.org/web/20221024160629/https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/why-nato-countries-don%E2%80%99t-share-cyber (accessed 10.24.22).

Thales, 2016. Thales to build "Cyber Range", a cybersecurity training and testing facility for the Dutch Defence Cyber Command [WWW Document]. URL http://web.archive.org/web/20221029095814/https://www.thalesgroup.com/en/worldwide/press-release/thales-build-cyber-range-cybersecurity-training-and-testing-facility-dutch (accessed 10.29.22).

Turčaník, M., 2020. A Cyber Range for Armed Forces Education. Inf. Secur. 46, 304–310. https://doi.org/10.11610/isij.4622

Ukwandu, E., Farah, M.A., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., Bellekens, X., 2020. A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. Sensors 20. https://doi.org/10.3390/s20247148

United Nations, 2021. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. United Nations.

Urias, V.E., Stout, W.M.S., Van Leeuwen, B., Lin, H., 2018. Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper, in: 2018 International Carnahan Conference on Security Technology (ICCST). Presented at the 2018 International Carnahan Conference on Security Technology (ICCST), pp. 1–5. https://doi.org/10.1109/CCST.2018.8585460

U.S. Cyber Command, 2021. DOD's Largest Multinational Cyber Exercise Focuses on Collective Defense [WWW Document]. URL http://web.archive.org/web/20221029103330/https://www.defense.gov/News/News-Stories/Article/Article/2863303/dods-largest-multinational-cyber-exercise-focuses-on-collective-defense/ (accessed 10.29.22).

U.S. Embassy in Slovenia, 2020. U.S. Strengthens Collaboration with Slovenia on Cybersecurity with New Cyber Range [WWW Document]. URL http://web.archive.org/web/20221029084128/https://si.usembassy.gov/u-s-strengthens-collaboration-with-slovenia-on-cybersecurity-with-new-cyber-range/ (accessed 10.29.22).

Zetter, K., 2014. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishers.