THE CYBER DEFENSE REVIEW
In press, 8 pages
https://doi.org/10.55682/cdr/7sc9-jf8s

SENIOR LEADER PERSPECTIVE

Playing the Future: Insights from Wargaming Cyber Conflict

Dr. John Curry*

Bath Spa University, UK

This piece explores how cyber warfare is evolving by combining professional wargaming with analysis of real-world cyber incidents. It highlights the lessons that have emerged from iterations of wargames about actual and potential cyber conflicts. As cyber conflict lacks the rich campaign histories available for conventional war, repeated wargaming of past operations is used to understand attacker intent, capability, and effectiveness. Several consistent patterns emerge across two decades of state-level cyber activity, including strategic signaling, integration with wider political and military campaigns, a focus on critical infrastructure, and the concentration of major cyber operations at the start of conflict. Looking ahead, the paper argues that while cyber capabilities are becoming more significant, they will take decades—and multiple major conflicts—to mature into a dominant class of weapons. A key strategic challenge is mobilizing national cyber power, particularly given the concentration of expertise in the private sector. Effective mobilization requires pre-planned public–private integration, cyber reserves, and extensive peacetime wargaming. It concludes that despite technological advances, human expertise remains the decisive factor in cyber conflict; wargaming is an essential part of developing these people.

Keywords: cyber warfare, cyber operations, state-sponsored cyber activity, wargaming, cyber wargaming, strategic cyber trends, national cyber power

* Corresponding author: j.curry@bathspa.ac.uk

Dr. John Curry is a Reader in Cyber Security and Professional Wargaming, Bath Spa University, UK. He is Co-Editor of the MORS Wargaming Journal and helped launch it. He teaches on MORS courses in Washington and is the Assistant Dean MORS Wargaming (Europe). He is also the Editor of The *History of Wargaming* Project (www.wargaming.co), which includes an active blog and YouTube channel (@HistoryofWargaming) dedicated to the history, theory, and practice of professional wargaming. Dr. Curry has published over one hundred books on various aspects of wargaming, including being the editor for the second edition of Peter Perla's (2022) *Art of Wargaming*.

INTRODUCTION

When people ask what I do, I often answer with a deliberately enigmatic reply: "I play strange games, with strange people, in strange places." What I really mean is that I use the discipline of wargaming as a structured method for studying the past, making sense of the present, and exploring how the future might unfold. In professional practice, a wargame is far more than a game: it is an integrated model that brings together aims and objectives, capabilities and orders of battle, resources, time and space, physical terrain, human factors, and the ever-present role of chance. It is a way to synthesize complexity so that decisions, behaviors, and outcomes can be examined within a realistic and coherent framework. Wargames are also a safe place to fail, as there are no real-world consequences to exploring the cyber battlefield within a game world.

Talking confidently about the future of cyber warfare is difficult because there is no established body of campaign histories to draw on. Incidents such as Russia–Estonia (2007), Russia–Georgia (2008), China–Philippines (2012), and the successive Russia–Ukraine campaigns from 2014 onward offer useful case study material, but they have not yet been synthesized into the kind of systematic campaign analyses that exist for conventional wars. If one wanted to study a hypothetical attack on Finland, the natural instinct would be to turn to the Winter War and Continuation War of 1939–40 and 1944, where enduring lessons (e.g., the constraints of narrow axes of advance and impact of extreme climate) still resonate. In cyber conflict, however, there is no equivalent canon: the analytical literature on past cyber campaigns is sparse, fragmented, and rarely integrated into broader strategic trends.

The academic theoretical literature has no clear narrative. Clarke and Knake's (2010) influential book suggested that America was facing a modern-day cyber threat equivalent to Pearl Harbor. The book successfully raised the profile of cyber. Thomas Rid's (2013) book *Cyber War Will Not Take Place* argued that while important, cyber will never be a decisive tool of warfare. In some ways, the academic narrative has hardly moved on from these opposing positions.

Faced with sparse, fragmented accounts of past cyber operations, I turned to repeated wargaming of real-world case studies as a way to build a clearer picture. I examined what the attackers were trying to accomplish, the capabilities they brought to bear, and how effective those capabilities actually were. I focused on the choices available to senior decision-makers, while also exploring the alternative courses of action they might have taken. Running these games again and again often generated

more questions than answers—for example, how long it would realistically take to develop bespoke malware for a specific piece of critical national infrastructure. In that sense, the games became tools for exposing the gaps in my understanding and highlighting where deeper analysis was needed.

CYBER WARGAMES

When I co-authored a working paper in 2014 on initial thoughts on cyber wargaming with Major Tom Mouat MBE (the UK's premier professional wargamer), we were surprised to find practically no activity in this area in the professional wargaming space. After publishing something, we were invited by various organizations to contribute to the development of cyber wargaming practice.

Most people involved in defense have at least a mental outline of wargaming, whether digital or manual. Wargaming involves a map representing the military geography, which is populated with military units. Known metrics are used to determine rates of movement, combat outcomes, etc. Some games have well-defined, rigid rules, while others, where umpires are available with current combat experience, allow more flexibility in determining outcomes based on the umpire's knowledge.

Cyber is now a part of some of these modern professional wargames (Curry and Drage 2021; Smith III, Kollars, and Schechter 2023). Often, cyber capabilities are abstracted away; for example, the *Rapid Campaign Analysis Tool* (RCAT) [1] used by the British military gives each side a certain number of 'cyber points'. Each capability costs a certain number of points; for example, a cyber recce costs 1 point, and disabling the enemy air defense radar costs 3 points. While this offers modest learning benefits about potential capabilities, it does not capture the complexity of the cyber battlespace.

A better way of wargaming cyber is to represent cyber capabilities using structured capability cards, as illustrated in Table 1. These kinds of tools help move cyber wargaming beyond abstract 'cyber effects' and toward a more realistic exploration of operational decision-making.

Table 1. Example Attributes for Cyber Capability Cards Used in Wargaming

Attribute	Description
Threshold for use	Political, legal, or rules-of-engagement conditions required before the capability can be authorized.
Escalation risk	Likelihood that the operation could trigger unintended escalation or provoke retaliation beyond the intended scope.
Host environment	Location or infrastructure from which the capability is deployed, including potential attribution implications.
Delivery vector	Mechanism used to gain access to the target.
Payload and intended effect	Operational objective or intended impact of a successful cyber weapon, such as disruption, deception, data exfiltration, physical damage, or information manipulation.
Stealth and detectability	Probability that the capability remains undetected before or during execution.
Resilience and persistence	Likelihood that the capability survives defensive responses once discovered, or can continue functioning within a contested environment.
Operational duration	Estimated period during which the capability is expected to remain viable or effective after deployment.
Collateral effects	Risk of unintended consequences affecting civilian systems, allied networks, third parties, or neutral actors.
Historical precedent	Comparable real-world cyber operations or incidents that help inform assumptions regarding effectiveness, detectability, and likely outcomes.

1. https://www.professionalwargaming.co.uk/RCAT-Longley-Brown-Smith.pdf

Designing capability cards for a cyber wargame is a useful exercise in itself and can be done at a low level of classification. Whether a potential cyber attack is possible is usually known (within the closed world of cyber security); whether someone has the capability today, or if they did, would they use it, is what should be classified at the highest level. This means that detailed attacks can be discussed for the purposes of a wargame, without disclosing whether the capability currently exists in a nation state's 'ready use' cyber weapons.

The purpose is not perfect technical simulation, but a more credible representation of the strategic trade-offs surrounding cyber capabilities. Even simplified capability cards can force players to confront the ambiguity and trade-offs that characterize real-world cyber conflict. Repeated gameplay across historical scenarios consistently highlighted several recurring dynamics of cyber conflict.

LESSONS FROM WARGAMING THE HISTORY OF CYBER CONFLICT

The historical record of cyber warfare is thin compared to that of conventional warfare. One way to explore this gap is to create wargames of significant cyber conflicts, such as Estonia (2007), China vs. Philippines (2014), Russia vs. Ukraine (2014-). Repeated gameplay with a wide variety of people from the IT industry, academics, penetration testers, postgraduates, etc., helps map the conflict space and, just as importantly, identify alternatives. Repeated gameplay drew out certain lessons.

Once hostilities begin, defenders rapidly harden their systems—patching vulnerabilities, changing passwords, tightening firewall rules, restricting data flows, and often uncovering malware already in place. Any cyber capability the attacker fails to employ early risks becoming obsolete as the target network evolves. This is why the initial wave of cyber-attacks is usually the most intense, and why the likelihood of long-dormant malware remaining undetected falls sharply once a state is on high alert. Decision-makers are incentivized to deploy capabilities early in a conflict due to rapid obsolescence once defenses adapt.

Another finding was the general optimism about the time it takes to generate new offensive cyber capabilities during a conflict. Most cyber weapons are difficult to design, sustain, and deploy. The Lockheed Martin cyber kill chain captures this through its missile metaphor, though not all operations follow that pattern; some rely on purchased criminal tools or insider access. Well-run networks are built to frustrate intruders and are continuously monitored and adapted, meaning that penetrating them can take months—or may never succeed at all. Unless a conflict is an existential threat to the nation-state, some of the private companies necessary to help develop a particular attack may not prioritize the state's requirements over their day-to-day operations.

An attacker's arsenal can be imagined as a hand of cards available at the start of a conflict. If those cards are not played quickly, some will be lost as defensive changes render them ineffective. New cards appear only slowly and unpredictably, leaving the attacker with a gradually diminishing set of viable options.

Players soon realize that DDoS is a key cyber weapon. The rise of DDoS-for-hire services has lowered the barrier to entry, allowing even inexperienced actors to participate in state-linked or politically motivated campaigns. Even a minor actor, if well-funded, can hire access to large AI-driven IoT botnets to create more adaptive, persistent ones that are difficult to counter. An ally, even if geographically distant and with limited initial cyber capabilities, can provide support by hiring additional capacity

to create a surge in attacks. The games routinely found that civilian supply chains were particularly vulnerable. Military hardware is hard to hack, but merchant ships, ports, trucks, and factories in the supply chain are not. One of the recurring questions identified but outside the scope of the games to answer was how the state can direct the IT industry to focus on protecting key areas necessary to sustain the war, but at the expense of other areas of the economy.

From the Operational to the Strategic Level

Perhaps the most interesting use of cyber wargames was to move from the operational to the strategic level. In a 2025 wargame about a conflict between North and South Korea, North Korea used cyber weapons to help make up for the weakness in its conventional forces. In the initial game briefing, South Korea and its allies were told about previous North Korean cyber-attacks, which used 'a large amount of pings' to overwhelm and crash the target's computer networks. During the game, North Korea hinted that its offensive cyber capabilities were largely limited to DDoS attacks. The initial briefing, combined with the actions of North Korea, conditioned the other side to only expect more DDoS-type attacks. The US and its allies did not exactly change their behavior, but they did not take the opportunity to strengthen their cyber capabilities. They expected North Korea to launch a cyber-attack in 'the same old way' and then they would defeat it in 'the same old way'. North Korea only revealed its advantage when the malware embedded in South Korean and Japanese military servers was activated, causing chaos. This gave North Korea a short-term military advantage (a boost to their combat rolls in game terms) while the other side cleaned the malware from their military computers and rebooted them. The South Koreans and Japanese could have potentially detected this attack (with a successful action and subsequent dice roll) if they had focused on scanning their computer networks for evidence of hostile actors.

In game terms, the North Koreans had used a covert action through the game facilitators. In the post-game debrief, the player from Japan highlighted his team's application of Sun Tzu's rules about deception, classical military theory applied to the 21st century! Here, the game demonstrated how easily prior assumptions about an adversary's capabilities can narrow defensive thinking.

Cyber Wargaming as a Tool for Operational Awareness

Sometimes, the junior members of the military have a perception that cyber is something dealt with at a higher level and is less applicable to them. Cyber operations can have real-world consequences, including loss of life, despite earlier academic arguments that cyber risk was largely theoretical. During the early stages of the 2014–2015 fighting in Ukraine, cyber activity contributed to the destruction of a large share of Ukrainian artillery. A Ukrainian officer had created a smartphone app that dramatically sped up targeting, reducing the time guns were exposed to counter-battery fire. After the app was promoted online and distributed informally, Russian operators compromised the download site and released an altered version. The modified app functioned normally but also transmitted the user's GPS coordinates, enabling Russian forces to locate and strike Ukrainian positions. The underlying malware was not identified until 2016.

Revealing to players in a tactical wargame—one not centered on cyber operations—that their routine peacetime social-media activity can enable long-range targeting in wartime delivers a powerful training effect. The apps on their phones could, quite literally, put their lives at risk.

Uncertainty, Friction, and Misperception in Cyber Conflict

Cyber wargames, like all wargaming, can convey the wrong training messages. One area in particular to be covered in the after-action game review is that not all the cyber capabilities in the game may be available for operations at a given moment. The mental model of some players was apparently that cyber weapons are built and then stored for years in a digital warehouse, ready for war. Cyber weapons, like all military tools, are shaped by circumstance and chance. Their effects can vary widely, and even well-designed operations can produce outcomes far from what planners intended. The impact of a cyber-attack is notoriously difficult to forecast.

An illustration is Israel's 2007 Operation Orchard, in which Syrian air-defense radars reportedly went dark during the final phase of an Israeli strike. The shutdown has been attributed to a covert, remotely activated "kill switch" embedded in the radar network. Yet the success of that operation rested on fragile conditions. Had the malware been discovered and analyzed beforehand, Syria would have been alerted to the impending attack and placed its air defenses on maximum readiness—almost certainly increasing Israeli losses. A routine software update could also have removed the implant or blocked the activation signal, allowing the Syrian system to function normally.

A second example comes from Russia's 2015 attack on Ukraine's power grid. The operation succeeded in cutting electricity to roughly 230,000 people for several hours, but forensic analysis later showed that the attackers had intended far more destructive effects. Their malware attempted to disable safety systems and create conditions that would injure operators and destroy substation equipment when power was restored manually. That escalation failed because of a simple programming mistake: the malware used incorrect IP addresses. The attack caused disruption, but it did not achieve the crippling outcome the planners sought.

These cases highlight the inherent uncertainty of cyber weapons. Sometimes they work precisely as intended; sometimes they misfire; sometimes they produce consequences far beyond what was expected. And at times, they fail in ways that inadvertently protect the target. Cyber wargames need to convey this uncertainty. Clausewitz captured this enduring truth when he observed that "*War is the realm of chance. No other human activity gives it greater scope.*" The digital domain is no exception: cyber operations are subject to the same unpredictability, friction, and human error that shape every other form of warfare.

One area where cyber wargames have had a notably lesser impact on training was in the information warfare domain. Information has always been a weapon in war, used alongside physical force to rally one's own population, reassure allies, and weaken the resolve of an opponent. My experience of games shows that senior leaders, such as politicians and their advisors, are masters at shaping the narrative during peacetime, and many of their innate skills transfer directly into wartime messaging.

FUTURE CYBER WARFARE

Cybersecurity now rivals the traditional defense sector in its ability to argue for ever-larger budgets, often accompanied by marketing that promises to "solve" an organization's cyber problems. Yet increased spending alone will not resolve the underlying challenges. History shows that genuine technological revolutions in warfare— poison gas, aircraft, tanks, drones—required sustained, state-level

investment and took years to mature. Cyber capabilities are growing in importance, but it will likely take decades and several major conflicts before they may become a dominant class of weapon in their own right.

A central challenge for senior leaders is harnessing the full cyber potential of the nation-state during an ongoing conflict. The United States partially demonstrated this in 2022, with Microsoft, among others, helping Ukraine rapidly migrate critical government systems to the cloud, preventing Russia from crippling the state by striking a handful of physical data centers. Without that shift, Ukrainian civil society would have faced severe disruption if the Russians had targeted the small number of physical data centers within Ukraine used by the Ukrainian government in the opening days of the war.

The UK faces a comparable challenge. GCHQ may have only a few hundred specialist cyber operators, while the private sector possesses far greater depth—there are probably more accredited penetration-testing firms in the UK than there are cyber staff at GCHQ. Major cybersecurity vendors such as CrowdStrike and global technology companies like Microsoft employ thousands of security professionals. In any conflict in which an adversary can rapidly mobilize its multinational technology base through pre-planned mechanisms, Western governments must be able to align their domestic high-tech industries with national defense needs just as quickly. That kind of mobilization framework has to be designed, tested, and refined through iterative cyber wargaming in peacetime, not improvised under the pressure of an actual war.

Modern states rely almost entirely on private companies to operate critical national infrastructure. This creates a difficult balance: government must help industry prepare for sophisticated threat actors without revealing sensitive intelligence that would compromise national security. At the same time, businesses must strengthen their resilience without overspending to the point of losing competitiveness to rivals—especially foreign competitors that invest less in cybersecurity, enabling them to deliver cheaper products. As discussed above, it may be necessary for the civilian economy to focus on protecting certain areas, even if it makes other sectors potentially more vulnerable. These sensitive topics are better explored in cyber wargames behind closed doors before the day real-world action is necessary.

Information warfare is now a core element of modern conflict, yet the people most skilled at shaping narratives—journalists, brand strategists, marketing professionals, influencers—sit entirely outside the machinery of the state. Any serious national strategy, therefore, needs a way to draw on this civilian talent through some form of cyber reserve or auxiliary force. Such a force would have to operate very differently from traditional military reserves, built around flexible engagement, civilian expertise, and rapid mobilization rather than uniformed structures. Regular cyber wargames are essential to integrate this diverse community with national objectives and to ensure that, in a crisis, they can be brought into a coherent information-operations framework. With British understatement, this can be challenging.

THE HUMAN ELEMENT

I will close this opinion piece by turning to the question of people. Wargaming should be an essential part of actively developing human expertise through practice. Wargaming is not only an analytic

tool, it is a powerful training instrument for senior leaders as well as the cyber warriors engaged in battle through the keyboard. Cyber wargames allow decision makers to experience simulated uncertainty, test assumptions, and rehearse complex coordination within the safe-to-fail environment of a game. Tightly focused cyber wargames, focused on decision-making rather than the 'deep geekery' of the staggeringly complex cyberspace, can be invaluable for helping bridge the communications gap between cybersecurity professionals and senior leadership. The general rule is that the longer the game, the less senior the participants are.

Wargames add value as part of the training cycle. There is strong evidence that a game's environment encourages participants to share experiences. For example, concluding a company-level cyber game with a short, brutally honest lecture by someone from another company who was hacked has an educational impact that is hard to match. The act of building a cyber wargame is an accepted way of exploring complex problems and is a form of applied research.

State-level cyber conflicts are complex; wargames are an established way of visualizing such complex problems in a single model. They are a particularly useful way of training decision makers in a non-judgemental environment, where they can test ideas. Playing wargames can be part of developing leaders' mental agility to cope when faced with the unexpected in crises. Participating in a game can be an essential part of team building as preparation for a crisis. Although Estonia's senior leaders had not played cyber wargames, no one had at that point, the fact that they played golf together meant they were a formed team when Estonia was on the receiving end of the first state-level cyber-attack. A less obvious point is that games are an invaluable way of developing an understanding of the opposing side's ('Red Team') perspective. The value of this should not be underestimated, as a better understanding of other stakeholders' world view can help prevent a crisis from inadvertently escalating.

Ultimately, cyber conflict remains a profoundly human contest shaped by leadership, adaptation, and decision-making under uncertainty. Advanced hardware and software may detect, block, and contain attacks, but it is human expertise in the cybersecurity world that designs, deploys, configures, monitors, and continually improves these systems. In the end, it is people who stop intrusions, because it is people who outthink the attackers. The real strategic challenge is how to attract, retain, and lead the rare individuals with the mindset and skills to do this work well. Wars are ultimately decided by human capability, and cyber conflict is no exception.

REFERENCES

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Ecco.

Curry, John, and Nick Drage. 2021. *The Handbook of Cyber Wargames: Wargaming the 21st Century.* Independently Published.

Perla, Peter. 2022. *The Art of Wargaming: A Guide for Professionals and Hobbyists.* Edited by John Curry. Originally published in 1990 by Naval Institute Press.

Rid, Thomas. 2013. *Cyber War Will Not Take Place.* Oxford: Oxford University Press.

Smith III, Frank, Nina Kollars, and Benjamin Schechter, eds. 2023. *Cyber Wargames: Research and Education for Security in a Dangerous Digital World.* Jefferson, NC: McFarland.