

JOURNAL OF ADVANCED MILITARY STUDIES

# JAMS

Vol. 16, No. 2, 2025



# The Lawful Losers?

## Why Democracies Struggle to Deter Cyber Aggression

Paul A. Eisenmann

---

**Abstract:** Democratic states are increasingly vulnerable in cyberspace due to inherent ethical constraints, transparency requirements, and legal oversight, significantly hindering their ability to effectively deter cyber aggression. This article critically assesses the strategic disadvantages democracies face using the examples of the United States, the United Kingdom, and Germany, including attribution challenges, threshold ambiguities, and the problematic diffusion of cyber capabilities among state and nonstate actors. It evaluates how strict adherence to international humanitarian law (IHL) further constrains democratic responses, contrasting sharply with the operational flexibility enjoyed by authoritarian adversaries. The article advocates strengthening cyber resilience, promoting global norm-building initiatives, and crucially retaining credible traditional military retaliation options. This integrated strategy enables democracies to uphold their values, effectively counter cyber threats, and actively shape global cyber norms, thereby ensuring strategic stability and digital security.

**Keywords:** cyber deterrence, democratic constraints, attribution, international humanitarian law, cyber norms, kinetic retaliation, cybersecurity resilience

### The Tension between Cyber Deterrence and Democratic Values

**A**s cyberspace increasingly becomes a domain of strategic competition, democracies confront unique and formidable challenges in deterring cyber aggression. Unlike conventional warfare, cyber operations blur

---

Paul A. Eisenmann is a PhD student serving as a junior officer in the German cyber command. He holds a master's in cyber security from the University of Portsmouth and a bachelor in history from the Open University in the United Kingdom. The views expressed in this article are solely those of the author and do not necessarily reflect the official position of the Kommando Cyber- und Informationsraum, the Bundeswehr, the German Federal Ministry of Defence, or the government of the Federal Republic of Germany. <https://orcid.org/0009-0005-8474-3454>.

*Journal of Advanced Military Studies* vol. 16, no. 2

Fall 2025

[www.usmcu.edu/mcupress](http://www.usmcu.edu/mcupress)

<https://doi.org/10.21140/mcu.j.20251602004>

the traditional boundaries of attribution, thresholds, and proportionality, leaving states uncertain about appropriate responses and vulnerable to miscalculations.<sup>1</sup> Democracies, bound by transparency, ethical accountability, and legal oversight, find themselves particularly disadvantaged compared to authoritarian states that can exploit these ambiguities without equivalent constraints. Consequently, democracies struggle to establish credible deterrence, often resorting to defensive postures or limited diplomatic sanctions that adversaries view as insufficient or negligible.

This article critically explores why democracies face these struggles and proposes actionable strategies to overcome inherent disadvantages. It investigates how ambiguities surrounding attribution and thresholds complicate deterrent measures, the structural inequalities in cyber capabilities between democratic and authoritarian states, and the problematic diffusion of cyber capabilities among state and nonstate actors. Furthermore, the article examines how strict adherence to IHL and ethical norms, while essential for democratic legitimacy, significantly constrains effective responses to cyber threats.

This article adopts a focused comparative analysis of three liberal democracies—the United States, the United Kingdom, and Germany—as illustrative cases of advanced cyber powers operating under distinct legal and constitutional constraints. These states were selected because they combine significant cyber capabilities, global security roles, and formal commitments to international humanitarian law, yet embody differing constitutional structures and strategic cultures. The United States operates with a strong executive and globally expansive cyber posture; the United Kingdom integrates cyber capabilities into joint operations under a parliamentary system with limited legislative oversight; Germany, constrained by the *Grundgesetz* (Basic Law), maintains a resolutely defensive stance under strict parliamentary control.<sup>2</sup> Examining this variation within a small set of capable democracies allows for sharper identification of how attribution burdens, threshold ambiguity, and IHL obligations interact to shape deterrence outcomes. The aim is to generate conceptual insights into the structural disadvantages democracies face in cyberspace, rather than to claim statistical generalizability across all democracies. Accordingly, all findings and conclusions in this article are scoped to the United States, the United Kingdom, and Germany. While some dynamics may be relevant to other democratic states, no claim is made that the patterns observed here apply universally across all democracies without further empirical examination.

Addressing these strategic vulnerabilities, the article ultimately argues for a balanced yet robust deterrence framework. While advocating for strengthened defensive resilience and international norm-building initiatives, it firmly underscores the necessity of retaining traditional military retaliation options—such as targeted kinetic strikes—under clearly defined and internationally agreed legal

frameworks. This comprehensive approach aims to enable democracies not only to defend their digital infrastructures and institutions effectively but also to shape a secure, stable, and norm-governed cyberspace environment.

### **Attribution, Ambiguity, and Thresholds**

Attribution, ambiguity, and thresholds are central challenges in cyber deterrence, presenting strategic, operational, and technical difficulties that democratic states must navigate carefully. Attribution, or correctly identifying the source of a cyberattack, remains technically and politically challenging due to the inherent anonymity and transnational nature of cyberspace.<sup>3</sup> This examination of democratic approaches—specifically those of the United States, the United Kingdom, and Germany—reveals their struggle with both technical constraints, such as false-flag operations and sophisticated obfuscation, and strategic constraints arising from the political risks of misattribution. For example, the United States has historically embraced “instrumental ambiguity”—a deliberate vagueness about thresholds, red lines, and response options intended to preserve decision-maker discretion and complicate an adversary’s risk calculus—to maintain flexibility, avoiding premature attribution that could force an escalation or damage diplomatic relations.<sup>4</sup>

For the three democratic states in this investigation, ambiguity in cyber engagement rules compounds the challenge of attribution by further constraining an already limited set of lawful and ethical response options. The North Atlantic Treaty Organization (NATO) explicitly recognizes that a cyberattack can trigger Article 5, which defines an attack on one member as an attack on all, yet its Cyber Defense Pledge strategically avoids specifying clear thresholds.<sup>5</sup> NATO’s ambiguous stance is intended to prevent adversaries from identifying precise red lines, thereby maintaining operational flexibility and deterrence through uncertainty. However, this ambiguity also creates opportunities for adversaries to conduct cyber operations below the threshold of armed conflict, exploiting the uncertainty around what constitutes a sufficiently severe cyberattack to trigger collective defense, as emphasized in Martin C. Libicki’s study on crisis and escalation dynamics in cyberspace.<sup>6</sup> While some scholars argue that strategic ambiguity can reduce the risk of automatic escalation by preserving political discretion, the cyber domain’s low visibility and rapid tempo often mean that adversaries perceive hesitation rather than resolve, thereby undermining deterrence rather than strengthening it.<sup>7</sup>

National doctrines further complicate this threshold ambiguity. The United States’ *2023 Cyber Strategy of the Department of Defense* emphasizes cyber operations below armed conflict thresholds to deter adversaries without escalating into conventional warfare, thus reflecting a careful calibration informed by constitutional principles of proportionality and necessity.<sup>8</sup> Similarly, the UK’s

Ministry of Defence outlines cyber capabilities as integrated into broader military operations, emphasizing adherence to IHL and ethical standards derived from British legal norms.<sup>9</sup> Germany, whose Basic Law prioritizes defensive strategies and mandates strict parliamentary oversight of military engagements, established the Cyber and Information Domain Service within the *Bundeswehr* (Federal Armed Forces), balancing operational effectiveness with legal accountability, as reinforced by Germany's *National Security Strategy*, which stresses a “resolutely defensive cyber stance” grounded in democratic oversight, parliamentary control, and a commitment to international law.<sup>10</sup> Thus, while national doctrines reflect an awareness of cyber threats, democratic states' internal legal and ethical frameworks severely limit their operational flexibility compared to authoritarian adversaries who face fewer normative constraints.

Operational constraints significantly influence these strategies. The U.S. Cyber Command's initiatives, like the Cyber Operational Readiness Assessment Program, aim to provide clarity and operational readiness within strict ethical and legal boundaries.<sup>11</sup> Likewise, the UK's National Cyber Security Centre employs active defensive measures under its Active Cyber Defence program, designed to mitigate threats within accountability frameworks under the oversight of publicly elected politicians.<sup>12</sup> These oversight mechanisms, while fundamental to a functioning democracy, puts additional constraints and bureaucratic burden on the agencies responding to cyber threats—defensive and offensive. Germany's Federal Office for Information Security highlights persistent high-threat environments and stresses enhanced resilience through technical preparedness and public-private collaboration.<sup>13</sup>

This reflects that, for the United States, the United Kingdom, and Germany, the intersection of attribution challenges, strategic ambiguity, and uncertain thresholds significantly complicates cyber deterrence. Addressing these issues requires continuous refinement of operational capabilities and legal frameworks to balance effectiveness, legality, and ethical accountability within their respective democratic systems.

## **Inequality in Cyber Capabilities**

The deployment of offensive cyber capabilities by democratic states presents profound ethical, legal, and strategic dilemmas, fundamentally conflicting with core democratic principles such as transparency, accountability, and adherence to the rule of law.<sup>14</sup> Democracies rest on open governance and oversight, wherein executive actions, particularly those involving military capabilities, must be transparent enough to permit public debate and legislative oversight. However, offensive cyber operations typically necessitate secrecy and operational ambiguity, challenging these fundamental tenets.<sup>15</sup> As Bryan Nakayama cautions, “the offensive employment of information operations risks deepening the challenges

that democracies currently face,” particularly by expanding state power in ways that are difficult to monitor or contest.<sup>16</sup> The absence of transparency consequently erodes public trust, creating a governance paradox where democracies use nondemocratic means ostensibly to protect democratic freedoms.

Moreover, offensive cyber operations are structurally weakened in the three democratic systems of this article, either by procedural drag or political backlash. In systems with strong legislative oversight, operational agility suffers.<sup>17</sup> For instance, Germany’s *Grundgesetz* mandates strict parliamentary oversight of military operations, especially offensive cyber operations, which must navigate legal gray zones that constrain flexibility and undermine the operational effectiveness required for timely and covert responses.<sup>18</sup> Conversely, when offensive cyber activities are primarily directed by the executive, they risk bypassing democratic checks, which can erode public trust and legitimacy. The United States exemplifies this tension: the executive branch frequently uses existing legal authorities expansively, leading to operations that evade detailed congressional review.<sup>19</sup> Similarly, the UK’s National Cyber Force, though subject to limited parliamentary scrutiny, has prompted concerns about the appropriate balance between secrecy and democratic accountability.<sup>20</sup> Thus, democratic regimes face a dual vulnerability: either offensive cyber operations become sluggish and bureaucratically encumbered, or they provoke domestic criticism for circumventing transparency and oversight.

Further complicating these operational challenges, offensive cyber operations occupy an uncertain legal and ethical landscape. Current IHL and existing treaties offer only a general framework for cyber warfare, leaving states—particularly the democracies in this investigation—to interpret foundational principles such as proportionality, necessity, and discrimination amid significant ambiguity.<sup>21</sup> The inherently diffuse and unpredictable impacts of cyberattacks raise ethical questions about civilian harm and collateral damage, which are critical under democratic legal frameworks. Democracies also risk setting troubling precedents: the use of intrusive tools such as malware or spyware for offensive purposes—even if targeted at adversarial entities—can inadvertently normalize practices antithetical to democratic ideals like privacy and freedom of speech. The Brookings Institution emphasizes that the creeping normalization of surveillance and disruption tools could erode civil liberties domestically, as the boundaries between legitimate security measures and authoritarian practices become increasingly indistinct.<sup>22</sup> In contrast, authoritarian states face fewer ethical constraints, as their populations are already subject to pervasive digital surveillance and coercive security practices; consequently, these regimes possess greater operational familiarity with intrusive cyber capabilities, conferring them a strategic advantage in potential conflict scenarios.

Strategically, reliance on offensive cyber capabilities also entails substantial

risks of escalation and unintended conflict, particularly troubling for democracies committed to maintaining international peace and stability. The ambiguity intrinsic to cyber operations complicates attribution, increasing the potential for misinterpretation and erroneous retaliation.<sup>23</sup> Such uncertainty may escalate tensions, thereby contradicting democratic states' strategic interests in global stability and predictable international behavior. Given that democracies typically maintain open and digitally integrated infrastructures, these states paradoxically become uniquely vulnerable to retaliatory cyberattacks, potentially inviting devastating consequences far exceeding the initial benefits of offensive cyber engagements. Consequently, offensive operations risk undermining national security rather than enhancing it, compelling democratic states to carefully weigh such tactics against their broader strategic imperatives and commitments to international peace.

These contrasts have practical consequences for deterrence credibility. The United States' willingness to engage in persistent cyber contact operations can signal resolve but also risks normalizing low-level hostilities, potentially eroding escalation thresholds over time.<sup>24</sup> The United Kingdom's emphasis on "responsible cyber power" strengthens normative legitimacy but can create operational hesitancy in crises where rapid offensive action might deliver strategic effect.<sup>25</sup> Germany's defensive posture preserves legal and political legitimacy at home and abroad, yet its highly restrictive authorization process may reduce the deterrent value of its cyber forces by making timely retaliation appear unlikely to adversaries.<sup>26</sup> Together, these variations underscore that even within a small group of high-capability democracies, institutional design and strategic culture can materially shape how deterrence is perceived and contested in cyberspace.

To align cyber policies with democratic values, states should emphasize transparency, clear legal frameworks, and international cooperation rather than opaque offensive strategies. Clearly codified legal structures under strict legislative oversight can bridge the accountability gap, helping to preserve democratic integrity and public trust even amid necessary secrecy. Initiatives promoting international cyber norms and cooperative cybersecurity frameworks, such as Microsoft's proposal for a "Digital Geneva Convention," underscore democratic states' commitment to ethical cyberspace conduct, emphasizing civilian protection and international accountability mechanisms.<sup>27</sup> While the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* constitutes a notable effort to adapt traditional legal principles to cyberspace, it remains fundamentally limited by its NATO-centric origins and lack of formal endorsement by global institutions like the United Nations or the International Committee of the Red Cross (ICRC).<sup>28</sup> Even among NATO members, significant differences persist regarding the permissibility and ethical scope of offensive cyber operations, with countries like the United States favoring a broader interpretation

of lawful cyber force while others, such as Germany, adopt a more restrictive and defensive posture. This divergence further weakens the manual's normative authority and highlights the urgent need for democracies to invest in truly multilateral frameworks if they intend to shape durable, widely accepted cyber norms. Strengthening cyber defense capabilities, international collaboration, and education in cyber resilience would enable democracies to uphold their values while effectively countering cyber threats. Such a balanced approach allows democratic states to assert leadership in setting global norms, ensuring both national security and democratic integrity in the complex digital age.

### **Diffusion between (Non)state Actors in Cyberspace**

Building on the challenges democracies face in establishing and enforcing international cyber norms, the diffusion of cyber capabilities between state and nonstate actors has significantly altered the operational dynamics of cyberspace, complicating traditional distinctions between organized military activities and actions taken by independent entities. Increasingly, states employ nonstate actors—such as private cybercriminal organizations, patriotic hackers, or loosely organized digital militias—to conduct cyber operations aligned with national interests, thereby maintaining plausible deniability and obscuring direct attribution. Russia, notably, has harnessed cybercriminal networks and informal hacking collectives in support of geopolitical objectives. Groups like KillNet and XakNet have launched cyberattacks against states supportive of Ukraine, while also soliciting cryptocurrency donations to fund activities in Russia's favor, often under the guise of volunteerism or patriotic activism.<sup>29</sup> Such state-backed proxy operations blur lines of accountability, challenge traditional methods of attribution, and complicate diplomatic responses to cyber aggression.

Simultaneously, nonstate actors have independently adopted tools and methods historically reserved for state-led cyber operations, enhancing their ability to inflict substantial damage and influence international conflicts. A prominent example includes the IT Army of Ukraine, a civilian-led digital force established in response to Russia's illegal invasion. Comprising thousands of volunteer hackers worldwide, this group has conducted coordinated cyber operations targeting Russian state entities, illustrating the empowerment of nonstate groups through democratized cyber capabilities.<sup>30</sup> This convergence in techniques and technology access reflects a broader diffusion phenomenon, enabled by readily available "turnkey" hacking tools—prepackaged software solutions that lower the technical barriers for sophisticated cyberattacks. As Mohamed Aly Bouke and Ahmed Abdullah argue, the widespread availability of these tools democratizes access to powerful cyber weapons, thereby empowering diverse actors ranging from organized crime syndicates to politically motivated hacktivist groups.<sup>31</sup> Unlike nuclear weapons, whose proliferation is

constrained by technical, material, and international regulatory barriers, cyber capabilities diffuse rapidly and uncontrollably across state and nonstate actors, making traditional nonproliferation approaches largely ineffective in the digital domain. While the diffusion of nonstate cyber capabilities poses risks to both democratic and authoritarian states, the challenge is qualitatively different for democracies. Authoritarian regimes can employ rapid, extrajudicial measures against suspected cyber actors, operate without public disclosure, and mobilize state-aligned proxies without domestic legal repercussions.<sup>32</sup> Democracies, by contrast, are bound by due process, evidentiary standards, and parliamentary or judicial oversight, which slow attribution, limit covert reprisals, and require public justification for countermeasures.<sup>33</sup> This asymmetry means that when nonstate threats operate in the legal or technical gray zone, democracies face higher procedural thresholds to act, greater public scrutiny if mistakes are made, and narrower operational windows before deterrent effects degrade. In effect, the same diffuse threat landscape imposes heavier strategic and political costs on democracies than on nondemocracies.

This dual diffusion—state actors appropriating nonstate entities and nonstate actors adopting state-level cyber capabilities—poses severe challenges to existing legal frameworks and democratic accountability structures. The complex interdependency between states and nonstate actors complicates the enforcement of international norms, making it difficult to clearly attribute cyberattacks and implement proportionate responses.<sup>34</sup> Democracies struggle to develop effective deterrence mechanisms in this ambiguous environment, as traditional diplomatic or military retaliation becomes problematic without unequivocal evidence linking adversaries directly to cyber operations. Consequently, this diffusion increases risks of miscalculation and escalation, particularly problematic for democracies committed to international law and conflict deescalation. The decentralized and diffuse nature of nonstate cyber entities makes diplomatic resolution challenging, as these groups lack formal organizational structures or accountability mechanisms typically available to state-controlled military forces. Without clear attribution or mechanisms to engage these nonstate actors diplomatically, democracies find themselves constrained, facing escalatory risks with limited options to manage crises effectively or peacefully.<sup>35</sup>

Addressing these challenges requires democracies to refine their strategic doctrines, emphasizing cyber resilience, attribution capabilities, and enhanced international cooperation. Effective international norms must explicitly address the roles and responsibilities of both states and nonstate actors, recognizing the diffusion and democratization of cyber capabilities. Democracies must foster clearer norms around state responsibilities in managing relationships with cyber proxies, explicitly prohibiting tacit support for nonstate actors engaged in offensive cyber operations. Strengthening cooperative international frameworks,

such as those proposed in initiatives like the “Digital Geneva Convention,” can establish clearer accountability standards, thereby mitigating the risks associated with this diffusion phenomenon and enhancing global cyber stability.

## **Ethical and Legal Constraints under International Humanitarian Law**

Democratic states adhering strictly to IHL face significant strategic and operational disadvantages in cyber warfare compared to authoritarian or noncompliant states, due primarily to ethical and legal constraints inherent in democratic systems. These disadvantages manifest specifically through the difficulty of attribution, the challenge of maintaining proportionality and distinction, and the underdeveloped legal frameworks governing cyber operations. Unlike conventional warfare, where the identity of an aggressor, the target of an attack, and the boundaries of battlefield effects are typically clear, cyber warfare is characterized by profound ambiguity and complex jurisdictional challenges, complicating the lawful execution of cyber operations.<sup>36</sup>

A central constraint is the principle of attribution, which is fundamental in determining lawful responses under IHL. Cyber operations frequently obscure the identity of attackers through sophisticated techniques such as routing attacks via multiple jurisdictions, hijacking civilian networks, or employing false-flag strategies, making attribution highly challenging.<sup>37</sup> While conventional military attacks usually provide immediate and reliable indicators of their source—such as identifiable military units or the geographical origin of artillery fire—cyberattacks rarely leave clear forensic evidence sufficient to justify immediate military response under the rigorous standards of democratic legal oversight. This lack of clear attribution severely limits democracies’ lawful retaliatory options, often restricting them to defensive or nonmilitary responses even when facing severe provocations.<sup>38</sup>

Additionally, the principle of distinction, requiring clear differentiation between military targets and civilian objects, is particularly difficult to uphold in cyber operations due to the interconnected nature of digital infrastructure. The ICRC has emphasized that because civilian and military infrastructures frequently overlap in cyberspace, targeting even a seemingly legitimate military objective can inadvertently disrupt essential civilian services such as hospitals, banking systems, and water supplies, causing disproportionate civilian harm.<sup>39</sup> In contrast, conventional warfare typically allows a clearer separation of military objectives from civilian infrastructure, simplifying adherence to IHL principles. Consequently, democracies that would strictly enforce compliance with the principle of distinction would find themselves strategically constrained. In particular, Germany vigorously has promoted IHL adherence as a central element of its foreign policy and therefore could see itself refraining from aggres-

sive cyber operations for fear of inadvertent violations of international law and humanitarian standards.<sup>40</sup>

Similarly, proportionality—the balance between anticipated military gain and potential civilian harm—poses complex ethical and operational challenges in cyber warfare. Cyber operations inherently carry risks of cascading and unpredictable effects, potentially causing extensive collateral damage beyond intended military targets.<sup>41</sup> For example, a targeted cyberattack intended to disable a military communication system could unintentionally incapacitate civilian telecommunications, healthcare services, or critical infrastructure. Such unintended outcomes conflict directly with democratic commitments to minimize civilian harm, creating a significant ethical and legal deterrent against aggressive cyber responses.<sup>42</sup> Conversely, conventional military methods, such as precise kinetic strikes, usually allow more predictable damage assessments and therefore clearer compliance with the principle of proportionality under established IHL guidelines.

Furthermore, democratic states face substantial disadvantages due to the underdeveloped international legal frameworks specifically governing cyber operations, contrasting markedly with the robust treaties and established norms present in conventional warfare. Currently, no comprehensive treaty explicitly addresses cyber warfare, leaving states reliant on interpretations of existing IHL principles developed for conventional kinetic conflicts. The ICRC highlights the resulting legal ambiguity, noting that without precise and universally accepted standards tailored explicitly to cyber warfare, democratic states are forced into cautious interpretations of IHL, restricting their capacity to execute effective offensive cyber responses.<sup>43</sup>

This legal ambiguity contrasts significantly with conventional warfare scenarios, where robust frameworks such as the Geneva Conventions provide clear standards and universally accepted rules governing state conduct, responsibilities, and liabilities. For example, the criteria defining an armed attack or the conditions triggering the right of self-defense under Article 51 of the United Nations Charter are much clearer and widely recognized for physical attacks.<sup>44</sup> In contrast, determining when a cyber operation constitutes an armed attack remains contested internationally, resulting in legal uncertainty and caution among democratic states adhering strictly to international law. Such uncertainty often compels democracies toward defensive postures or diplomatic solutions, limiting their ability to use decisive cyber actions proactively, thereby handing strategic advantages to less scrupulous adversaries who exploit these ambiguities.<sup>45</sup>

Moreover, the transnational nature of cyberspace further complicates adherence to and enforcement of IHL. Cyber operations can originate, transit, and impact multiple jurisdictions simultaneously, complicating attribution, prose-

cution, and enforcement efforts significantly more than conventional military engagements, which typically remain geographically contained.<sup>46</sup> This inherent complexity poses severe jurisdictional and diplomatic challenges for democratic states seeking lawful responses or accountability through international cooperation or prosecution.<sup>47</sup> Authoritarian states or non-state actors operating with implicit state consent exploit these legal gaps, conducting aggressive cyber campaigns from jurisdictions where legal enforcement by democratic states proves impractical or diplomatically costly.

In summary, democratic states' strict adherence to IHL significantly disadvantages them in cyber warfare relative to conventional military engagements due to attribution challenges, complexities around proportionality and distinction, underdeveloped legal frameworks, domestic accountability mechanisms, and jurisdictional issues. Addressing these critical disparities requires the international community, guided by organizations such as the ICRC and relevant think tanks, to develop explicit and robust international norms and treaties tailored specifically to cyber warfare. Until then, democratic states remain strategically constrained, compelled to balance ethical compliance against operational necessity within an ambiguous and rapidly evolving cyber domain.

### **How Can We Get Global Norms in Cyber Warfare?**

The urgent need for global norms in cyber warfare stems from the unique characteristics of the digital domain: anonymity, asymmetry, and the lack of inherent territorial boundaries. Unlike conventional military domains, cyberspace currently lacks a widely accepted and enforceable framework to regulate state behavior. Although efforts like the United Nations' Group of Governmental Experts and the Open-Ended Working Group have confirmed that existing international law, including IHL, applies to cyber operations, these initiatives have fallen short of creating binding agreements or comprehensive enforcement mechanisms.<sup>48</sup> Democratic states, which traditionally anchor their military actions within clear legal and ethical boundaries, find themselves particularly vulnerable in this regulatory vacuum.

Building global norms in cyber warfare will require a multipronged strategy focused on broadening participation, increasing transparency, and forging common interests even among geopolitical rivals. Initiatives like the Global Commission on the Stability of Cyberspace and the Paris Call for Trust and Security in Cyberspace represent important steps toward establishing baseline expectations, particularly the protection of critical civilian infrastructure and prohibitions against indiscriminate cyberattacks.<sup>49</sup> However, these efforts face resistance from authoritarian states that perceive cyber operations as indispensable asymmetric tools to counterbalance Western technological advantages.<sup>50</sup> Moreover, unlike nuclear nonproliferation frameworks where material con-

straints and verification mechanisms can physically limit the spread of capabilities, cyber weapons are often intangible, replicable, and difficult to monitor.<sup>51</sup> As Joseph S. Nye argues, deterrence and dissuasion in cyberspace must therefore rely more heavily on norm-building and reputational costs rather than purely on threat-based strategies.<sup>52</sup>

To foster truly global norms, democracies must expand multilateral engagement beyond traditional Western alliances, including regional organizations and emerging cyber powers. Transparency measures, such as voluntary disclosures of doctrine and restraint pledges, can help build mutual trust. Equally important is reinforcing the idea that sovereignty, civilian protection, and proportionality apply as much in cyberspace as in conventional conflict.<sup>53</sup> However, efforts toward transparency and normative restraint must be calibrated carefully, ensuring that democratic states retain sufficient operational flexibility until reciprocal commitments to norm-building are forthcoming from all major actors. Without sustained commitment to coalition-building, norm promotion, and credible mutual restraint, the digital domain risks further fragmentation into competing spheres of influence governed by conflicting cyber doctrines.

In this context, collective deterrence mechanisms enhance the credibility and capacity of democratic states to shape responsible behavior. Through alliances such as NATO, democracies can coordinate threat intelligence, pool technical expertise, and present a unified front against malicious cyber actors. The NATO Cyber Defense Pledge reflects this commitment, emphasizing not only mutual defense but also sustained national investments in cyber preparedness.<sup>54</sup> Institutions like the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) further contribute by advancing legal, strategic, and operational thinking. Most notably, the *Tallinn Manual 2.0*, produced under the auspices of the CCDCOE, remains the most comprehensive nonbinding attempt to clarify how existing international law applies to cyber operations—serving as a reference point for norm development, even if it has yet to gain universal traction.<sup>55</sup>

In conclusion, shaping global norms in cyber warfare requires democracies to move beyond deterrence thinking alone and toward proactive *norm entrepreneurship*, which means the active promotion and institutionalization of new rules, in this case responsible behavior in cyber warfare. Through inclusive diplomacy, targeted normative agreements, and the reinforcement of ethical cyber behavior, the international community can work toward a cyberspace governed by rules rather than brute force.<sup>56</sup>

## **Strategies for Ethical and Effective Cyber Deterrence**

While the establishment of global norms in cyber warfare remains an essential long-term objective, democracies must also adopt immediate strategies to

safeguard their digital domains ethically and effectively. Strengthening cyber resilience offers a pragmatic path forward, enabling states to uphold democratic values while countering escalating cyber threats.

A core element of resilience is a layered defense-in-depth strategy. Technological safeguards such as firewalls, intrusion detection systems, and regular vulnerability assessments help protect critical infrastructure. The U.S. *Cyber Resilience Review* offers a framework emphasizing operational continuity and adaptive response to evolving threats.<sup>57</sup> Equally essential is cybersecurity education. Enhancing cyber literacy among citizens and IT professionals reduces human error and strengthens societal resilience. Lydia Kraus et al. demonstrate the long-term value of embedding cybersecurity training in academic curricula, while Valdemar Švábenský et al. highlight the importance of cyber ranges and simulations for preparing personnel to respond effectively under pressure.<sup>58</sup> International cooperation further reinforces national efforts. NATO-led initiatives promote shared training, Joint exercises, and interoperable defense systems, fostering collective security among democracies.<sup>59</sup> National legislation also plays a key role: the UK's Cyber Security and Resilience Policy integrates resilience into public infrastructure strategy, ensuring legal frameworks keep pace with dynamic threat environments.<sup>60</sup>

Together, these elements form a comprehensive model of cyber deterrence by denial—one that disincentivizes attacks by reducing their potential impact and increasing the cost of success. Crucially, such an approach avoids the ethical pitfalls of offensive retaliation, aligning with democratic commitments to transparency, proportionality, and civilian protection. By investing in layered defense, human capacity, and cooperative policy, democratic states can strengthen cyber stability while maintaining legitimacy in the international system.

## **Leave Traditional Deterrence on the Table**

Given the escalating threat landscape in cyberspace, democratic states must decisively maintain the option of direct military action to effectively deter adversaries. Cyber aggression can no longer be answered solely through defensive cyber measures, diplomatic condemnations, or limited sanctions—responses that have repeatedly proven insufficient in curbing malicious cyber activities from strategic competitors. James M. Acton clearly illustrates how the absence of clearly defined thresholds and credible attribution emboldens aggressors, increasing the risk of inadvertent escalation.<sup>61</sup> Democracies, therefore, must demonstrate unequivocally that hostile cyber operations will trigger tangible, real-world military consequences.

Kinetic military actions, such as precision airstrikes or missile attacks on adversarial cyber infrastructures—including data centers, communication hubs, and operational command posts—must be firmly established as credible

responses within IHL frameworks. Laurent Gisel and Tilman Rodenhäuser underscore the urgency of explicitly applying IHL principles like proportionality and necessity to cyberspace conflicts.<sup>62</sup> Clearly articulated legal justifications for military retaliation will not only reinforce legitimacy but also strengthen deterrence by signaling serious consequences for cyber provocations. In parallel, democracies should aggressively pursue covert intelligence and special operations to dismantle adversarial cyber capabilities. Tim Maurer compellingly argues for the strategic impact of apprehending or eliminating state-sponsored cyber operatives.<sup>63</sup> Targeted intelligence operations that disrupt adversaries' cyber units and infrastructure send an unmistakable message: cyber aggressions will incur personal and operational risks. While some democracies possess the military reach and legal latitude to credibly threaten kinetic responses to cyber aggression, others—such as Germany—are more constrained by constitutional limits, parliamentary oversight, and force projection capacity. This analysis therefore confines its discussion of conventional military options to states, like the United States and the United Kingdom, whose political and military frameworks make such measures viable and would call upon defense-passive and reactive states like Germany to rethink its overall deterrence strategy in light of the illegal Russian invasion of Ukraine.

In conclusion, to preserve strategic stability and safeguard democratic institutions, states must adopt a robust deterrence posture that explicitly includes direct and decisive military retaliation for cyber aggression. Allowing nations like China and Russia to conduct cyber operations without severe repercussions only encourages further hostility. A deterrence strategy that integrates clear military options within existing legal frameworks is vital to maintaining global security and deterring future cyber threats.

## **Conclusion**

Democratic states currently face significant strategic disadvantages in cyber deterrence, primarily due to their adherence to ethical constraints, transparent governance, and rigorous legal frameworks. These inherent limitations create a challenging operational environment, where attribution remains difficult, thresholds remain ambiguous, and offensive actions risk escalating into broader conflicts. To overcome these issues, democracies must combine immediate defensive strategies—such as strengthening cyber resilience and fostering international cooperation—with the credible threat of traditional kinetic retaliation under explicit IHL frameworks. Moreover, democracies must lead efforts to establish global cyber norms through inclusive diplomacy, clear transparency measures, and concrete accountability standards. While pursuing these norm-building initiatives, democratic states should remain pragmatic, maintaining flexible and credible military options to ensure adversaries clearly un-

derstand the real-world consequences of cyber aggression. These conclusions are drawn from the specific institutional and strategic contexts of the United States, the United Kingdom, and Germany and should be understood within that comparative frame. By strategically balancing defensive resilience, proactive norm entrepreneurship, and decisive traditional deterrence, democracies can effectively protect national security interests, uphold democratic values, and promote global cyber stability. Without these integrated measures, the digital domain risks further fragmentation and heightened vulnerability to cyber threats.

---

## Endnotes

1. Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies* 46, no. 3 (2021): 534–69, <https://doi.org/10.1080/01402390.2021.1944856>.
2. The *Grundgesetz* has served as the Federal Republic of Germany's constitution since 1949. *Cyber Capabilities and National Power*, vol. 2 (London: International Institute for Strategic Studies, 2023).
3. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, nos. 1–2 (2015): 4–37, <https://doi.org/10.1080/01402390.2014.977382>.
4. Benjamin Jensen and Brandon Valeriano, *What Do We Know about Cyber Escalation?: Observations from Simulations and Surveys* (Washington, DC: Atlantic Council, 2019).
5. NATO, "Cyber Defence Pledge," press release, 8 July 2016.
6. Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: Rand, 2013), <https://doi.org/10.7249/MG1215>.
7. Jacquelyn G. Schneider, "Deterrence in and through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Erik Gartzke and Jon R. Lindsay (New York: Oxford University Press, 2019), 95–120, <https://doi.org/10.1093/oso/9780190908645.003.0005>.
8. *Summary: 2023 Cyber Strategy of the Department of Defense* (Washington, DC: Department of Defense, 2023). At the time of this article's writing, the official name of the Department of Defense had not yet changed to Department of War.
9. *Cyber Primer*, 3d ed. (London: Ministry of Defence, 2022).
10. *National Security Strategy* (Bonn, Germany: Federal Ministry of Defence, 2023).
11. *Summary: 2023 Cyber Strategy*.
12. *Active Cyber Defence: The Sixth Year* (London: National Cyber Security Centre, 2023).
13. *The State of IT Security in Germany in 2023* (Bonn, Germany: Federal Office for Information Security, 2023).
14. Nori Katagiri, *How Liberal Democracies Defend Their Cyber Networks from Hackers: Strategies for Deterrence* (Cham, Switzerland: Palgrave Macmillan, 2024), <https://doi.org/10.1007/978-3-031-54561-0>.
15. *Guidance: Responsible Cyber Power in Practice* (London: National Cyber Force, 2023).
16. Bryan Nakayama, "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations," *Cyber Defense Review* 7, no. 3 (Summer 2022).
17. *Cyber Capabilities and National Power*, vol. 2.
18. Matthias Schulze, "German Military Cyber Operations Are in a Legal Gray Zone," *Lawfare*, 8 April 2020.
19. Nakayama, "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations."
20. Joe Devanny, "The Ethics of Offensive Cyber Operations," Foreign Policy Centre, 3 December 2020.

21. Maj Benjamin Ramsey, "An Ethical Decision-Making Tool for Offensive Cyberspace Operations," *Air and Space Power Journal* 32, no. 3 (Fall 2018): 62–71.
22. Ted Piccone, *Democracy and Cybersecurity*, Policy Brief (Washington, DC: Brookings Institution, 2017).
23. Rid and Buchanan, "Attributing Cyber Attacks," 4–37.
24. *Cyber Capabilities and National Power*, vol. 2.
25. Joe Devanny and Professor John Gearson, eds., *The Integrated Review in Context: Defence and Security in Focus* (London: Centre for Defence Studies, Kings College London, 2021).
26. Rid and Buchanan, "Attributing Cyber Attacks," 4–37.
27. Jeremy Hsu, "You Are the Target of Today's Cyberwar," *Wired*, 2 March 2017.
28. Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017), hereafter *Tallinn Manual 2.0*, <https://doi.org/10.1017/9781316822524>.
29. David Kirichenko, "Crypto Boosts Ukraine—and Russia," Center for European Policy Analysis (CEPA), 5 January 2024.
30. Matt Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," *Wired*, 27 February 2022.
31. Mohamed Aly Bouke and Ahmed Abdullah, "Turnkey Technology: A Powerful Tool for Cyber Warfare," arXiv.org, 28 August 2023, <https://doi.org/10.48550/arXiv.2308.14576>.
32. Katagiri, *How Liberal Democracies Defend Their Cyber Networks from Hackers*.
33. *Cyber Capabilities and National Power*, vol. 2.
34. Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, UK: Cambridge University Press, 2018), <https://doi.org/10.1017/9781316422724>.
35. Maurer, *Cyber Mercenaries*.
36. Kubo Mačák and Tilman Rodenhäuser, "Towards Common Understandings: The Application of Established IHL Principles to Cyber Operations," *Humanitarian Law & Policy* (blog), ICRC, 7 March 2023.
37. Maurer, *Cyber Mercenaries*.
38. "International Humanitarian Law and Cyber Operations during Armed Conflicts," *International Review of the Red Cross* 102, no. 913 (2019): 481–92, <https://doi.org/10.1017/s1816383120000478>.
39. "International Humanitarian Law and Cyber Operations during Armed Conflicts," 481–92.
40. *Cyber Capabilities and National Power*, vol. 2.
41. Schmitt, *Tallinn Manual 2.0*.
42. Robin Geiss and Henning Lahmann, *Protecting Societies: Anchoring a New Protection Dimension in International Law in Times of Increased Cyber Threats* (Switzerland: Geneva Academy of International Humanitarian Law and Human Rights, 2021).
43. "International Humanitarian Law and Cyber Operations during Armed Conflicts," 481–92.
44. Geiss and Lahmann, *Protecting Societies*.
45. Maurer, *Cyber Mercenaries*.
46. Mačák and Rodenhäuser, "Towards Common Understandings."
47. Maurer, *Cyber Mercenaries*.
48. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (New York: United Nations, 2015); and Arindrajit Basu, Irene Poetranto, and Justin Lau, "The UN Struggles to Make Progress on Securing Cyberspace," Carnegie Endowment for International Peace, 19 May 2021.
49. *Advancing Cyberstability: Final Report, November 2019* (The Hague: Global Commission on the Stability of Cyberspace, 2019); and "Paris Call for Trust and Security in Cyberspace," Ministère de l'Europe et des Affaires Étrangères (MEAE), November 2018.

50. Christian Ruh et al., *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads* (Washington, DC: Carnegie Endowment for International Peace, 2020).
51. Bouke and Abdullah, "Turnkey Technology."
52. Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 43, no. 3 (2017): 44–71, [https://doi.org/10.1162/ISEC\\_a\\_00266](https://doi.org/10.1162/ISEC_a_00266).
53. Laurent Gisel and Tilman Rodenhäuser, "Cyber Operations and International Humanitarian Law: Five Key Points," *Humanitarian Law & Policy* (blog), ICRC, 28 November 2019.
54. "Cyber Defence Pledge."
55. Schmitt, *Tallinn Manual 2.0*.
56. Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (Autumn 1988): 887–917, <https://doi.org/10.1162/002081898550789>.
57. *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide* (Washington, DC: Department of Homeland Security, 2014).
58. Lydia Kraus et al., "Want to Raise Cybersecurity Awareness?: Start with Future IT Professionals," in *ITiCSE 2023: Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education* (New York: Association for Computing Machinery, 2023), <https://doi.org/10.1145/3587102.3588862>; and Valdemar Švábenský et al., "Enhancing Cybersecurity Skills by Creating Serious Games," in *ITiCSE 2018: Proceedings of the 23d Annual ACM Conference on Innovation and Technology in Computer Science Education* (New York: Association for Computing Machinery, 2018), <https://doi.org/10.1145/3197091.3197123>.
59. Alexander Kott et al., "Approaches to Enhancing Cyber Resilience: Report of the NATO Workshop IST-153," arXiv.org, 20 April 2018, <https://doi.org/10.48550/arxiv.1804.07651>.
60. *Cyber Security and Resilience Policy Statement* (London: Department of Science, Innovation, and Technology, 2025).
61. James M. Acton, "Cyber Warfare & Inadvertent Escalation," *Daedalus* 149, no. 2 (2020): 133–49, [https://doi.org/10.1162/daed\\_a\\_01794](https://doi.org/10.1162/daed_a_01794).
62. Gisel and Rodenhäuser, "Cyber Operations and International Humanitarian Law."
63. Maurer, *Cyber Mercenaries*.