International Journal of Intelligence and CounterIntelligence, 0: 1–28, 2022
© 2022 Taylor & Francis Group, LLC
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2022.2081904

PERSPECTIVE

JD WORK

Burned and Blinded: Escalation Risks of Intelligence Loss from Countercyber Operations in Crisis

Abstract: As the limitations of purely defensive cyber operations continue to be demonstrated in the continuing pressure of hostile cyberthreats, the U.S. government has introduced new doctrine to shape countercyber operations (CCO) leveraging offensive options to degrade threat capabilities and infrastructure. Planners have only begun to understand the broader implications of these new concepts in difficult periods of crisis. The article explores the parallels to other strategic early warning and intelligence capabilities, surfacing distinctions based on the unique dynamics of cyberconflict to identify scenarios in which CCO successes may prove potentially destabilizing and lead to greater escalation risk.

INTRODUCTION

States leverage offensive cyber operations capabilities for multiple purposes, including as one aspect of a wider intelligence contest by which they seek to

JD Work serves as a Professor at the National Defense University, College of Information and Cyberspace. He holds additional affiliations with the Saltzman Institute of War and Peace Studies at the School of International and Public Affairs at Columbia University, the Krulak Center for Innovation and Future Warfare at Marine Corps University, and the Cyber Statecraft Initiative at the Atlantic Council. He can be found on Twitter @HostileSpectrum.

The views and opinions expressed here are those of the author and do not necessarily reflect the official policy or position of any agency of the U.S. government or other organization.

understand the diplomatic and military intentions, and plans, of a competitor. Sustained intrusion campaigns are documented by researchers, and attributed by industry and governments on a recurring basis, providing evidence of this ongoing activity in pursuit of states' espionage needs.[1] Identifying and defeating these intrusions is a routine task for defensive cyber operations elements. Yet these efforts have proven limited in the face of sustained adversary threat pressures, leading states and other actors increasingly to employ their own offensive capabilities in countercyber operations (CCO) intended to track, deny, and contest hostile intrusion access and supporting infrastructure.

CCO are given increased importance under the U.S. government's adoption of a new doctrine of persistent engagement, implementing a strategic shift to defend forward in cyberspace to contest hostile offensive cyber operations involving espionage and disruption of critical U.S., allied, and partner national infrastructure. This doctrine advances the proposition that engagements in the cyberenvironment are emerging as a new form of crisis interaction, where adversaries compete over initiative and position in order to access and hold at risk key sources of national power.[2] The doctrine developed as an alternative to the challenges in adapting earlier strategic approaches based on deterrence and coercion theories to the new warfighting domain in the first decades of operations.[3] From this doctrine arises the need to challenge adversaries that currently operate freely within compromised systems and networks, in order to reset the fundamental conditions of security within the environment.[4]

This is a difficult proposition in an environment that has generally been acknowledged to at least favor the offense, if not one that is offense-dominant (even as the contours of this balance remain debated).[5] New U.S. Cyber Command thinking acknowledges continued defensive countermeasures to secure systems and networks, and efforts to reduce vulnerabilities across the technology ecosystem—including through strengthened partnerships and improved liaison engagement for information sharing and collaborative missions to remediate compromised systems. However, it is the proposed employment of offensive cyber operations in defensive cyber operations response actions, and more broadly for CCO objectives, that deserves further attention.

There is, however, only limited discussion to date in the unclassified literature regarding the operational aspects that may result in escalation problems arising from countercyber actions under the persistent engagement doctrine. In part, this is likely because these problems—and the mechanisms by which they are mitigated—are relatively obvious to experienced offensive operators, planners, and their leadership. Yet there are an increasing number of parties newly arrived to the space who lack technical grounding, crucial mission context, and appropriate mental models by which to understand the contours of operations. This is especially notable when the topic is discussed in high-level conversations regarding comparative policy and strategy approaches. The further exegesis therefore may offer new utility toward resolving problems where operators and intelligence officers/analysts find themselves talking past policy staff and academic audiences. Additional consideration of these issues is also likely to improve the training and education of future cyberwarriors and those that support these missions through intelligence, capabilities development, and wargaming within the wider community of practice. It becomes further critical to understand the operational and strategic implications of this novel doctrine, especially as foreign allies now also consider the alignment of their own efforts in a similar manner.[6]

To such ends, this article proceeds in six parts. It first sets out the objectives of the countercyber mission and distinguishes this mission from similar countering problems. I next consider the frequently raised concern that such operations result in escalation, as adversaries react to lost capabilities or perceived threats to their positions. Generally accepted intelligence case histories of intelligence losses are identified, encompassing the loss of national technical means of early warning, loss of spies during mobilization, loss of signals intelligence due to sudden adversary emissions control, and roll-up of saboteur networks; and are mapped to parallel cyber incidents. I then propose a typology of possible CCO actions and associated reactions by adversary offensive cyberplanners. From these interactions, I offer a series of propositions to explain the dynamics of escalation that may arise from such operations. On the basis of these propositions, the article closes with a set of conclusions identifying how escalation risk may be reduced when considering intervention options.

The article offers conceptual contributions that identify and explain potential sources of escalation where hostile cyberespionage operations are degraded by CCO actions, illustrated through examples drawn from the empirical case record. This article also provides new theoretic contributions that outline principles for future operational design and execution intended to minimize potential flareback and escalation—principles that are also intended to form the basis of future research design and testing by analysts and intelligence studies scholars seeking to validate and expand on these contributions.

COUNTERCYBER MISSION

CCO actively seek to deny, degrade, disrupt, deceive, and destroy adversary offensive cybercampaigns. While these objectives may be expressed through a variety of language, depending on the year and the organizational or doctrinal alignment of the planners, the intent remains consistent.[7] States may leverage offensive cyber capabilities for a variety of espionage, sabotage, direct action, and operational preparation of the environmental objectives in anticipation of future conflict. While individual incidents involving compromise of specific target nodes may be more notable in open-source reporting, the proper unit of analysis to understand these activities is at the level of the campaign—where adversaries manage difficult tradeoffs of nondetection, persistence, management of scarce offensive capabilities, and effects outcomes.[8] CCO seeks to defeat adversary access, freedom of maneuver, and positional advantage for these campaigns—and in so doing, remove specific capabilities from the adversary's future options space, and arsenal.

These are explicitly operational-level objectives. If successfully executed, they limit adversary options and associated courses of action, serving to shape adversary behaviors. Accomplishing these objectives is often intended to change the balance of initiative between opposing forces. Success may change the timing of actions in ongoing engagements as well as shift potential future phases. Cumulatively, these impacts may alter operator, planner, and decisionmaker perceptions of ongoing exchanges. These operational objectives in turn may then connect to strategic-level outcomes. Such strategic outcomes may include deterrence (whether by denial, or by changing perceptions of risk and therefore punishment amid failing operations), or alternatively the emergence of tacit agreement toward more responsible behaviors.[9] But these strategic objectives differ from the operational interactions of ways and means—and the associated adversary reactions—that I consider in this article.

Concepts of operation for CCO may echo earlier parallels familiar to both air planners and counterintelligence professionals. Offensive counterair missions, and associated operations against ballistic missile targets, are superficially suggested when considering the domain. However, there are distinct differences that require these cyber operations to be evaluated on their own terms.

Cyberengagements, unlike air operations, are not defined by sorties. Nor are adversary capabilities assembled in fixed configurations within a common order of battle such as an air wing. These capabilities are not dependent on fixed inventories of commodities such as petroleum, oil, and lubricants that are subject to depletion-absent logistics replenishment on a deterministic schedule.[10] Rather, the employment of offensive cyber capabilities portfolios may involve operations over an extended period of time—either for espionage objectives or as operational preparation of the environment for future effects options. Even where capabilities are leveraged for prompt effects, they may leverage supporting infrastructure composed at point of need that leverage longstanding vulnerabilities and unaddressed exposures.[11]

Likewise, counterintelligence framing poses specific challenges that would burden CCO in a too narrowly restrictive model. Again, superficial similarities do exist. Further, some useful parallels may be considered in the detection of particularized intrusions by hostile intelligence services, and within the option space when defining objectives in turning, shaping, and degrading adversary access. However, CCO actions occur more broadly than within law enforcement context, or even the broader scope of a national intelligence organization's presence and activities, that typically defines counterintelligence as practiced to date. Counterintelligence practitioners have themselves criticized the narrowness of historical and contemporary practice, likely with a view toward an expanded remit.[12] In the absence of this established role, CCO therefore fall to other professionals within the distinct cyber mission. Opportunities for synergistic coordination between the disciplines are noted, however, in the conclusion of this article.

ESCALATION FEARS

Proposals to employ CCO options in order to relieve hostile pressure on defended systems are frequently challenged on the basis that any response actions conducted outside of one's own network—touching adversary infrastructure—may provoke escalation. Generally, existing scholarship finds that cyber operations do not commonly result in escalation.[13] However, the prospect is never far from the debate, informed by early and insightful work theorizing the trajectory of capabilities yet to fully mature.[14]

The challenges of escalation management within the context of proposed countering options under the doctrine of persistent engagement has been a key point of concern since the introduction of these concepts, and subject to continuing debate as the intellectual originators of the approach and the leadership that has adopted this thinking continue to seek to articulate their vision.[15] In part, this likely stems from the longstanding focus within the international relations community on the issues of escalation between states in competition and conflict across multiple domains—where extension of these ideas into the new operating environment is a natural line of thinking. The uncomfortable silence of professionals restricted from public discussion of classified matters has also complicated understanding of these issues, where key distinctions of operational art are missed and oversimplified generalizations lead to confusion over targets, actions on objectives, and effects assessment. There nonetheless remains a legitimate space of concern where the unknowns of these new concepts of operation intersect with complex adversary intelligence and military services, their associated contractor and proxy organizations, and the authoritarian regime leadership that directs the activities of these entities. A number of scholars have explored issues related to causal chains of escalation and associated feedback loops, rules of engagement considerations, emotional factors impacting escalation decisions, other higher-order effects that may drive escalation, concerns about differing adversary reactions to operations conducted at scale, cross-domain interactions leading to escalation, and the potential for both adversary and allied/partner perception and misperception of persistent engagement activities leading to inadvertent escalation.[16]

U.S. Cyber Command has even been accused, in both formal literature and informal discussion, of not having considered the potential for escalation involved in countering operations under the persistent engagement framework.[17] These concerns may have initially been valid given the early limited information about the doctrine that had been disclosed publicly, but increasingly are simply unfair, given that they are contradicted by direct testimony regarding leadership attention to the issue. [18] Evidence of such considerations as a key component of planning for offensive capabilities employment is documented in declassified operational materials released by Cyber Command from earlier engagements by Joint Task Force ARES against Daesh to counter violent extremist propaganda, recruitment, and other key activities—the most significant publicly acknowledged offensive cybercampaign acknowledged to date.[19] There is no reason to believe that such a crucial area of emphasis would be arbitrarily abandoned in subsequent missions where offensive capabilities were directed toward countering objectives—especially where Cyber Command leadership has emphasized the continuing utility and validity of this operational precedent as a model for future mission organization, coordination, and execution.[20]

It is important to note that escalation here is posited by critics both as the result of operational acts, involving the direct engagements of opposing forces on the wire, as well as through perceptions (and misperception) that may arise among observers and the decisionmakers to whom they report. Multiple factors may contribute to escalation decisions, interweaving operational realities, variable situational awareness, incompletely understood technical complexity, emotional responses, and flawed operational planning or execution. These factors may, however, be largely abstracted for the purposes of this analysis, which focuses on dynamics between the offensive actor and the countering responder (although further research to explore the relative impact of these factors would of course likely provide much value, as has been seen in other studies of escalation in differing domains). These dynamics arise from intersection of operational positions, extant capabilities, and relative initiative and are structural in nature.

PARALLELS IN ANALOGY TO INTELLIGENCE INTERACTIONS IN CRISIS

If one considers the interactions of offensive and CCO as a contest of intelligence, it is natural to look to prior parallels in intelligence studies that will offer insight into what are the particularly dangerous interactions between competitor states—particularly those that are in heightened states of tension or approaching conflict. Dynamics that might encourage escalation at these moments are particularly of concern when planning future operations, or when evaluating evidence of current operations. Even if not all operational choices, or potential countering courses of action, may drive escalatory outcomes there are almost certainly some subsets more likely to contribute to such concerns.

Intelligence history points to four potential parallels that may be considered analogies, where the loss of intelligence resources at a particularly critical moment may be dangerously destabilizing and may potentially lead to uncontrolled escalation. While it is recognized that analogies are difficult in cyber operations, they still remain a starting point to consider the problem space.[21] Upon this basis, scholars may then build better inferences derived from case evidence.

These four parallels were identified through a review of the Cyber Disruptions Dataset, encompassing more than 100 cases of operational disruption of adversary cyber operations through administrative, defensive, and CCO techniques.[22] Through these case studies, intelligence equities not accounted for in conventional consideration of disruption factors were identified for further analysis. While additional such equities are likely to be observed in future interactions, these parallels form a substantial starting point for framing relative value in contest.

Loss of National Technical Means of Early Warning

The first analogy is the parallel encountered when facing a sudden loss of early warning capabilities in a nuclear crisis. The role of national technical means, including overhead electro-optical and radar imagery, nonimaging infrared sensors, and over the horizon radar are acknowledged to have been crucial elements in stabilizing extended militarized competition between the Soviet Union and the West, especially the United States. The capabilities, reliability, and the repeatedly proven track record of these systems over the decades have removed much concern about potential undetected surprise missile attack—especially in the most common reference "bolt out of the blue" strategic nuclear scenarios. While this assurance remains always a matter that must be revalidated with every new generation of weapons systems, sensor architectures, and command and control models, it remains a foundational concept for warfighters, planners, and decisionmakers. It has therefore long been recognized that sudden and unexpected loss of these capabilities, and the assurance they provide, in times of crisis may be considered a strong indicator of conflict initiation.[23]

This has not stopped extensive consideration of the conditions under which offensive actions against early warning capabilities might be required, and of the various means by which such attacks may be carried out. Much of the development of military space control capabilities—including direct ascent antisatellite (ASAT) weapons, on-orbit engagement platforms, direct energy, and electronic warfare options must be evaluated against this backdrop. This is notable in Russian capabilities development from the Cold War through to recent maneuvers by the Russian Cosmos 2543 "inspector" shadowing the USA245 satellite, reported by open sources to be a KH-11 CRYSTAL imagery intelligence (IMINT) platform—and subsequent apparent testing of kinetic intercept capabilities.[24] Likewise, the People's Liberation Army has extensively explored options to target space-based assets—including explicit planning for actions against early-warning satellites, and realization of both high-energy laser and kinetic ASAT test events.[25] However, the longstanding debate over such actions in theory and in practice has extended the acknowledgment—in both explicit interactions and in tacit military preparations—that actions that may blind technical means to potential surprise attack are not to be taken lightly.

The analogy to CCO against active intrusion is immediately apparent. Indeed, the problem has been previously highlighted in scholarship examining potential escalation—notably by Jason Healey and Robert Jervis. These gentlemen argue that cyber interactions in crisis may be unexpectedly escalatory, especially as offensive cyber options are likely to be used early in the conflict, leading to a greater chance of miscalculation driven by the stronger first-use pressures in offensive-advantaged cyber interactions—particularly where intelligence failures have occurred.[26] Deliberate CCO that target adversary cyberespionage activities providing access against core leadership communications or strategic command and control architectures are of course then likely a matter of first objectives, intended to deny and degrade adversary intelligence. The sudden loss of accesses previously enjoyed by hostile intelligence organizations leaves a vacuum—which in less mature organizations, or in support of less experienced leadership, may thus be filled by the enemy's worst fears.

No direct case evidence for such analogies becoming manifest in CCO interactions has yet emerged. Similar scenarios have, however, developed in consideration of defensive cyber operations where adversary operators have achieved substantial access to core command and control, leadership, and intelligence communications. These have included the reported widespread compromise of U.S. military systems by operators attributed to the Russian

Federal Security Service in the early phases of the intrusion set tracked by industry variously under the cryptonyms Turla/VENOMOUS BEAR/IRON HUNTER, which drove U.S. government defensive response in Operation BUCKSHOT YANKEE. In this case, extensive penetration of U.S. government networks had presumably provided Russian intelligence services with aggressive visibility into current deployments, future planning, and policymaker thinking that would undoubtably provoke anxieties upon sudden loss after eviction.[27] Likewise, compromise of the Republic of Korea (ROK) wartime contingency planning by Democratic People's Republic of Korea (DPRK) cyberespionage may be considered, again leading to defensive countermeasures responses by ROK defenders to evict North Korean hackers from military networks.[28] The loss of extensive espionage-derived insights into South Korean (and by extension U.S.) military intentions fits this case—especially against the backdrop of ongoing tensions over the North's prohibited nuclear and ballistic missile programs.

However, to date, these cases are not publicly known to have incorporated active CCO— although one can immediately see the value such options would have played in these incidents. Neither of these examples proved escalatory—in no small part likely due to the lesser immediacy in the tensions between competitor states at the time of intrusion detection and defensive response eviction. Should an adversary have observed CCO interventions leading to the loss of access, one may consider that a potentially different reaction may have resulted.

Loss of Spies during Mobilization

Likewise, CCO that deny and degrade an adversary's ongoing cyberespionage access against competitor networks may be likened in analogy to the arrest or other loss of human agents in place prior to military mobilization. Intelligence history is replete with examples of assets tasked with espionage against preparations for movement, either by a state that may be readying to bring its forces to the field or by a state that will strike through invasion or other offensive action. In the early modern world, espionage focused on port and shipbuilding activities required for fleet mobilization—for example, in operations targeting Louis XIV's fleet at Toulon and Marseilles in the late 1690s.[29] In the industrial age, this espionage frequently targeted the railways enabling mass troop and materiel movements—such as in German and French espionage seeking to understand potential Russian troop movements against Turkey in 1887.[30]

Case evidence for such analogies having played out in real-world CCO interactions remains as yet difficult to document publicly. Nonetheless, a similar scenario may be seen in the SOLAR SUNRISE incident, in which U.S. military networks were compromised during a period of heightened tensions corresponding with mobilization for Operation DESERT FOX airstrikes in support of United Nations Special Commission (UNSCOM) nuclear inspections in Iraq. Initial attribution theories of this intrusion included potential action by Iraqi intelligence services, based on technical factors of previously known Iraqi access to at the time what were then limited Internet connectivity options routing through the United Arab Emirates. However, this attribution theory was incorrect, and the intrusion was subsequently linked to ego-motivated juvenile cybercriminals.[31] Again, this case resulted in only defensive cyber operations and law-enforcement response. It should be noted that this incident was among the earliest actions of the emerging cyber mission, and while the elements of the scenario are useful in considering analogy, improvements in attribution capability and countering capacity would likely mean future responses would differ markedly in contemporary engagement.

Loss of Signals Intelligence Due to Sudden Adversary Emissions Control

The third analogy is one that shifts perspective and agency from that of the actor-engaged CCO to the offensive operators whose targeted action is intended to be degraded or disrupted. An adversary who deliberately goes "radio silent" has long been recognized as a warning indicator suggesting imminent conflict. However, in practice, such observed indications are considered highly variable in potential severity due to the frequency with which emissions control may occur for various periods of time within a military or intelligence organization. The most severe analogies are the deliberate destruction of codes and cipher machines by diplomatic embassies. This is a historically grave step, not least of which given the challenges of provisioning new secure communications that are amplified in a time of crisis, in order to reverse this decision and restore routine channels. Intelligence history provides the analogous case of "Black Friday," where new Soviet communications security measures resulted in immediate loss of communications intelligence access as ciphers that had previously been subjects of successful cryptanalysis were replaced by new special purpose cipher machines and associated communications nets across the General Staff and military districts culminating on 29 October 1948.[32] This incident, occurring over a several-month period from at least August 1948, was sudden in intelligence terms but sufficiently delayed as to preclude immediate warning of war. The cooling off effects of rolling communications security implementation were further tempered by the lack of other source indications, and the American perceptions of nuclear superiority that would not be shattered until the detonation of the first Soviet nuclear weapon, RDS-1, the next year.

Adversary adaptation in cyber operations in order to defeat defensive cyber operations and intelligence campaign tracking is not unusual. Retooling after disclosure, or at some planned periodicity, or after some degree of operational degradation based on perceived exposure, is a common offensive operator behavior.[33] However, an offensive planner that becomes aware of countercyber pressure—especially where countercyber network exploitation is used to inform defensive detection and passive countermeasures—may regain the initiative through retooling, rebuilding fresh command, and control infrastructure, or shifting tactics/techniques/procedures (TTP).

Beyond routine disclosures driven by digital forensics and incident response or other defensive intelligence interactions, sudden or otherwise unexpected loss of offensive visibility to countercyber actions, particularly in a time of crisis tension, may lead to dangerous misinterpretation by immature analysts, planners, or leaders. This risk may be amplified as defender cyber intelligence functions detect renewed intrusion activity using new tooling, infrastructure, or TTP that may be attributed to prior adversary activity groups due to incomplete offensive refresh. Such renewed activity—particularly if an offensive operator is seeking to reestablish the scope and scale of prior access—may be mistakenly seen as intensification. Where such access extends further into sensitive networks or critical infrastructure systems than defenders may have been previously aware of—even if operators are merely restoring status quo ante—such behaviors may be further interpreted as escalation.

Real-world case examples of such interactions may include apparent countercyber intervention against the ATP28/FANCY BEAR/IRON TWILIGHT attributed VPNFilter botnet infrastructure operated by the Russian General Staff Main Intelligence Directorate (GRU).[34] In this case, however, the risk of adversary intensification or escalation does not appear to have been realized in the absence of other critical external conflict factors at the time—despite ongoing tensions involving the Russian military occupation of territory in Ukraine. Subsequent apparent intervention against the CYCLOPS BLINK botnet infrastructure—assessed by multiple intelligence services as a successor to the VPNFilter codebase—in the period immediately preceding renewed invasion in February 2022 may also be considered.[35] Given Russian forces' apparent full commitment to preplanned actions attempting to seize Kyiv, it is difficult to assess any action here as escalatory in context of the immediate conflict dyad. (The question of escalation against wider North Atlantic Treaty Organization interests, in this case, being also as yet unresolved as the conflict continues.)

Roll-Up of Saboteur Networks

The fourth analogy that may be explored from intelligence history is the moment in which saboteur networks and other direct action elements are detected and interdicted (colloquially, rolled up) during crisis tensions. There are conditions in which defenders in the course of routine counterintelligence activities may become aware of potential adversary espionage and subversion, intended to provide hostile options for operational preparation of the environment.

While such scenarios are always of concern, crisis factors may lead to a more immediate and interventionist response than might otherwise be pursued in times of routine competition as defenders evaluate the potential for imminent damage to their interests. One can see these dynamics at work in a number of historical cases. In 1917, the destruction of military shipyards and vessels by Imperial saboteurs proved a serious threat to U.S. logistics on the eve of entry into World War I. [36] Likewise, Great Britain had long feared potential labor strikes fomented by German assets to disrupt trade and defensive preparations in advance of the war. [37] UK intelligence concern would further extend to potential foreign support to Irish Republican Army terrorism, focused particularly on potential direct action against rail chokepoints that might impede the movement of forces in response to a feared German invasion in 1943.[38] During the Cold War, Soviet services invested substantial effort into planning and preparation for direct action by intelligence and special forces elements intended for the opening hours of a war never fought in Europe. This concept of operations was famously profiled in novelist Tom Clancy's fictional depiction *Red Storm Rising*, in which a traffic accident led to the compromise of a *spetsnaz* element tasked with striking targets in Germany on the eve of a major armored offensive by Soviet troops.[39] However, these same playbooks were well demonstrated in reality during the invasion of Afghanistan in 1979, leveraging State Committee for Security (KGB) special purpose troops and GRU *spetsnaz* in a *desant* action to enable rapid seizure of power under operational plan STORM-333.[40] Similar tactical actions by "little green men"—irregular forces, private military contractors, and their GRU advisors—were observed in the Russian occupation of Ukrainian territories including Crimea in 2014.[41] A nearly identical concept of operations likely underpinned the immediate phase of the renewed invasion of Ukraine in February 2022, based on observed initial *desant* operations in the vicinity of Kyiv.[42]

CCO case examples fitting these analogies are likewise difficult to publicly document. However, parallels may be drawn in a few serious incidents. In 2016, the PATCHWORK/KATAR/MONSOON intrusion set reportedly compromised the personal security detail providing executive protection for a neighboring regional state's head of government.[43] Beyond the political intelligence value here, the potential kinetic implications of information acquired through such an intrusion are grave, particularly where they may involve advance knowledge of the movements of the principal. However, the incident was detected by third-party commercial cybersecurity researchers, and it is not known if the target state was aware of the incident. In any event, no disruptive countercyber action against this intrusion activity was noted. Yet, had such events transpired during a period of heightened tensions, and involved even a slightly different but yet still entirely plausible fact pattern, the potential escalation concerns are obvious.

Some degree of similar concern likely attaches to the compromise of White House communications networks attributed to Russian intelligence services reported publicly in 2014, although the extent of this intrusion was likely more limited and would have offered less substantial insights into presidential movements around which a greater degree of classification control is presumably exercised.[44] North Korean attributed HIDDEN COBRA/ LAZARUS offensive operators were observed leveraging lure documents associated with, and potentially seeking to compromise, information related to Presidential Special Mission aircraft and Executive Flight Detachment units. [45] This incident must likely be considered as triggering a much higher degree of risk—particularly against the backdrop of tensions between North Korea and the United States during the spring of 2017. Yet, even in this case, escalation was not noted——suggesting an even greater degree of tension, or less ambiguous indications of intent, as the true threshold for escalation risk.

INTERACTIONS BETWEEN CCO AND OFFENSIVE CYBER ESPIONAGE AND OPERATIONAL PREPARATION OF ENVIRONMENT CAMPAIGNS

Even as case evidence remains immature due to the paucity of CCO to date, analogies and their substantiating indications remain sufficient to permit the first outlines of potential interactions between CCO actions against offensive campaigns to be drawn. One may systematically consider the following types of CCO actions relevant within the potential scenarios in which potential higher risk of escalation must be evaluated. These represent only a subset of the full spectrum of CCO options within the action and reaction space corresponding to the above-described parallels.

Burn, and Overtly Attribute

CCO engagement against an adversary offensive cybercampaign results in public disclosure and attribution, including potential "name and shame" operations. Known cases of such activities to date have included CCO targeting APT29/COZY BEAR/IRON HEMLOCK.[46]

Burn and Leak, through Third-Party Commercial Intelligence Disclosure

CCO engagement results in compromise of ongoing adversary offensive operations, and resulting visibility is used to drive attribution and campaign tracking by commercial and other industry cyberintelligence activities. The disclosure in the 2014 burning of the Careto/Mask intrusion set attributed to the Spanish national intelligence service, and the 2014 disclosure of the Machete/Andromeda intrusion set attributed to the government of Colombia, may potentially be considered as examples of such cases.[47] More recently, the April 2022 disclosure of the PIPEDREAM/INCONTROLLER malware that was designed to deliver destructive effects against industrial control systems may also provide an example. While first known to have been publicly described by commercial intelligence services, multiple government agencies joined in providing coordinated warning and technical analysis.[48] This case is particularly unusual in that the payload was reportedly found and recovered before its operational deployment.[49]

Burn and Leak, through Third-Party Covert Influence Disclosure

CCO engagement compromises adversary offensive campaigns but information related to these campaigns is selectively leaked via third parties. Such publication may result in disclosure of malware and other intrusion tooling, identification of active intrusion infrastructure, as well as information leading to organizational and individual attribution. Western media reporting suggests that at least some part of disclosures in 2019 burning APT34/OILRIG/HELIX KITTEN/COBALT GYPSY/CHRYSENE intrusions, attributed to the Iranian Ministry of Intelligence and Security, resulted from such deliberate covert action measures.[50] However, media coverage of these alleged interventions lacks the clarity needed to distinguish this case more comprehensively.

Burn, Detected by Adversary after Deliberate CCO Clandestine Signaling

In some instances, no public acknowledgment of a CCO action may be observed. The adversary becomes aware of the impact to their offensive campaigns only by deliberate messaging—such as through explicit communication to operators within a command and control infrastructure or another closed environment, or demonstrative action across other live architectures—intended to serve clandestine signaling purposes. While intrusion set operators are unlikely to disclose that such messaging has occurred, leading to a lack of real-world case examples, law-enforcement botnet takedowns have used extant command and control channels to notify victims of remediation options. This was notable in the case of the Bredolab/Oficla spam infrastructure disruption in October 2010.[51] Such messaging was presumably also observed by the adversary and could be therefore limited only to adversary nodes.

Burn, Detected by Adversary Due to Loss

Not all actions intended to deny or degrade adversary offensive operations may be immediately understood by those conducting the campaigns in question. In particular, threat activity at scale typically involves a series of otherwise routine frictions and failures that must be overcome to sustain a campaign effectively over time against normal changes to target system and network configuration, even before considering defensive countermeasures. CCO pressures may therefore only be noticed by an adversary at some threshold of loss. Under differing scenarios, it may be possible that the adversary will not understand the cause and origin of the loss, while in other circumstances, the manner and scope of loss may be unmistakable. A recent case example is provided where an Iranian-aligned attribution front known as the Jerusalem Electronic Army, involved in active intrusion campaigns attempting to sabotage Israeli critical infrastructure networks, publicly acknowledged disruptive and destructive CCO impact to the group's technical infrastructure.[52]

Burn, Failed Attempt at CCO Intervention

Sometimes even the best planned and executed CCO options may not result in substantive impact to degrade or deny adversary offensive capabilities. Such failures may result from a variety of operational, technical, or timing factors. In some subset of failure cases, adversary intrusion sets may become aware of CCO pressures and react even if the CCO objectives were not met. State-level CCO failures are even more poorly documented than other types of CCO actions. However, case examples may be observed in takedown actions against criminal infrastructure—including botnet activities reportedly also repurposed for official intelligence purposes by hostile foreign intelligence organizations, such as in the October 2015 failure of a disruptive action targeting Dridex/Bugat.[53]

From these various types of CCO actions, one may anticipate the following range of potential adversary offensive cyber planner reactions, in from least to worst possible escalation severity. Again, these do not encompass the full range of possible responses to any CCO, but rather follow directly from the earlier parallel scenarios and associated actions.

Surge Operations to Regain Access and Capabilities Positioning using Existing Tooling

An adversary seeks to restore prior options, either out of perceived crisis necessity or internal bureaucratic pressures driven by organizational culture, leadership demands, or similar common factors that drive programmatic decisions within military and intelligence services.

Surge Operations to Regain Access and Capabilities Positioning using Less Mature Capabilities

An adversary operator may substitute novel exploit and implant tooling to replace previously burned malware. There is the potential that these capabilities may not have undergone the same degree of operational test and evaluation. Such risk is of course magnified where adversaries do not conduct a formal assessment of new capabilities within controlled range environments complete with target representative components.[54] Likewise, operators and planners may be less familiar with these tools, and the edge cases where such tooling may produce unintended consequences or other collateral damage across complex target systems and networks. Even where adversaries may have previously sought to pursue a degree of responsibility in the conduct of offensive cyber operations, time pressures may lead to operator or developer errors, or other failure modes.[55] These failures in turn may lead to escalatory conditions that more deliberate operations might have avoided.

Surge Operations to Innovate New Access and Capabilities Positioning

Regardless of the capabilities replacement approaches described previously, an adversary may choose to use these capabilities in new ways not previously seen in an effort to acquire new options for employment in the context of the ongoing crisis. Such innovation is generally considered to require some degree of preoperational intelligence and planning effort, but in a complex and dynamically moving situation, there may often be fleeting opportunities that an adversary may recognize that can deliver unique value. Further, while careful targeting and deliberate effort to achieve access for longer-term persistence, with emphasis on capabilities that remain NOBUS (available to Nobody but US), is a hallmark of the "Western way" or even "American way" of offensive cyber operations, other adversaries may not place the same value on such characteristics.[56] Where such efforts involve targets an adversary has not previously pursued, or involve a higher probability of detection/effects maximized operational decisionmaking tradeoffs, it is more likely that these behaviors will be interpreted as intensification and escalation when and where they are observed.

Imminent Conflict Assumption

An adversary believes that war or other escalated conflict is likely in the near term, based on analogies to other intelligence interactions, and may execute preplanned courses of action for war initiation. In these scenarios, planner and operations management flexibility may be reduced as mobilization and opening salvo logics take hold and may force operations into more linear and more aggressive modalities than seen in operations employing dynamic decisionmaking processes while short of conflict.

PROPOSITIONS: DETERMINANTS OF ADVERSARY REACTIONS

Based on the scope of the outlined interactions, the following propositions may be advanced to describe key determinants of adversary reactions to CCO that disrupt, degrade, or deny their capabilities in a time of crisis.

The Reaction of Offensive Intrusion Set Operators Is Likely to be Shaped in Part by the Available Capabilities Inventory that Remains at Their Disposal Following CCO Impact

The depth of this magazine, and its quality, dictates options available to reacquire access, as well as the relative manner of employment in an immediate crisis. Beyond the immediate magazine, set reactions will likely be shaped by comparative capacity to retool new offensive capabilities within relevant timeframes of the crisis. The responsiveness and quality of the quartermaster—whether for organic capabilities development, or for contract or gray/black market acquisitions—will almost certainly factor into service and national leadership thinking when forced to confront sudden loss of espionage access or prepositioned offensive options.

Set Reactions Are also Highly Likely to be Shaped by the Experience of the Operators and Planners

Veteran actors will have previously encountered the inevitable setbacks that come with any operations in contact with an actively defended target network. Experienced teams will be familiar with the operational frictions imposed by routinely changing enterprise and operational technology environments, and will have previously gone through positional losses—including those that will dictate requirements for retooling and restoration of initial intrusion footholds. As a result, they are less likely to react out of emotion, or paranoia, and more likely to be deliberate in ways that are less escalatory unless deliberately directed by leadership. It is, however, the challenges of management, oversight, and overall program direction that may continue to pose risks in such a scenario. More senior decisionmakers may be unlikely to have the same degree of understanding, nor the same prior experiences, as the technical-level operators. The management of offensive teams may not always communicate clearly, or well, regarding the character of specific engagements within ongoing campaigns. This disconnect between what occurs on the wire, and how leadership makes sense of these events, poses the potential for miscalculation. This is further exacerbated by power distance dynamics between line operations elements and service or national leadership components, as well as a variety of command information channel problems. Many of these issues are familiar from other military domains, with disastrous outcomes noted in the historical record that offer substantial lessons here.[57]

Intrusion Set Reactions Are also Likely to be Shaped by the Degree of Overall Crisis Pressure

Both uniqueness of, and immediacy of loss, in impacted capabilities may be felt more keenly. One can outline a variety of scenarios in which essential elements of information, or prepositioned ability to hold at risk *schwerpunkt* or *systempunkt* nodes, were sought in requirements serviced by offensive cyber operations—but where such targets are less amenable to actions through classic clandestine espionage, national technical means of intelligence collection, or direct action.[58] Losses of capability in crisis are more likely to be seen as imposing grave risks where cyber options have taken on more prominent importance—whether due to paucity of human intelligence assets, lack of effective traditional signals intelligence options in radio frequency spectrum or public switched telephone networks, or limited utility of IMINT and other geospatial intelligence capabilities.

The Degree of Publicity Attending CCO Will Likely Influence Adversary Reaction

It is counterintuitive, but the more publicly that an intrusion set is burned the less likely it may be considered an immediate risk of escalation. Rational states are unlikely to focus on political jockeying over public perceptions of mere espionage where the intent is to engage in higher-order conflict, given the availability and utility of other better understood instruments for signaling—including military posture changes. While it is possible a state may attempt to leverage a very public intrusion incident as casus belli justification for kinetic retaliation or other options further along the escalation ladder, such a course of action necessarily involves steps that are distinct from the countercyber operations maneuver. These other measures may be distinguished from those in and through the networked environment, and considered through classic international relations concepts.

FROM PROPOSITIONS TO CONCLUSIONS

The identification of stability degrading or potentially escalatory factors in crisis interactions is not intended to argue generally against the conduct of CCO. It is unrealistic to assume any state will simply permit an adversary unfettered access to sensitive systems and networks, nor to rely solely on passive defensive options in challenging extant footholds or ongoing attempts to acquire new access. However, these factors should indeed be considered by potential planners and the management and oversight structures that approve new countercyber concepts of operations. If the above-noted propositions hold true, minimization of potential flareback and associated unintended consequences may be sought through deliberate choices in operational design and execution. Such planning considerations include the following principles: Extended corrosive degradation of adversary offensive capabilities under CCO pressure over time, as opposed to a sharp, immediate intervention, is anticipated to be less likely to provoke escalatory or other retaliatory actions. The extended attrition of capabilities removes from the equation the elements that may lead to the perception of catastrophic loss, reducing possible emotional factors as well as blunting adversary reaction cycles as internal bureaucratic processes are forced to repeatedly iterate through decision cycles around each progressive stage of degradation. This is magnified where the adversary may become aware of differing elements of attrition at varying points in time, with incomplete or even conflicting information about the events in question.

CCO effects executed through multiple causal mechanisms may be presumed to reduce chances of potential destabilizing outcomes. Single interventions are more likely to be identified by adversaries and give rise to negative reactions. Therefore, CCO executed through multiple mechanisms that vary in effect, scope, and timing (even if relatively closely sequenced) may corrode adversary capability and capacity without the adversary fully understanding the campaign as a distinct event that may spark retaliatory or escalatory response.

CCO may be further planned as shaping operations, where selective denial of adversary capabilities under specific circumstances serves to degrade overall offensive effectiveness, in order to protect specific higher value defender equities. Where an adversary may expect and understand countering as a single decisive action, the intermittent failure of attempted actions under differing conditions may be indistinguishable from normal operational friction for some time. Selective denial may also serve to help manage how and through what means an adversary reaction in and through cyberspace may play out, where countering planners may deliberately leave untouched some aspects of an adversary's offensive architecture, thereby making it more likely that hostile operators and their leadership will rely on this remaining capability in any retaliatory or escalatory response. This will in turn allow countering mission forces early warning of potential negative reactions, and the ability to blunt retaliatory impact. These concepts have recently gained traction within U.S. and allied Intelligence Community circles, particularly where outcomes are considered as an alternative to strategic objectives of deterrence.[59]

Deliberate deception and offensive counterintelligence options, distinct from but executed in coordination with CCO, may mitigate negative adversary reactions. Adversary threat activity groups of significance largely involve military and intelligence service organizations and their contractor or proxy assets. Where a sustained CCO campaign is ongoing over a distinct period of time, the ability of the adversary to recognize such pressure may be deliberately complicated by the introduction of deliberately misleading or ambiguous information into known collection channels. Penetration of hostile intelligence organizations may also be leveraged to delay assessment processes or even blunt the conclusions of such assessments by mishandling operational data or altering analytic judgment. Even where such options are not possible, a countering planner may seek to provoke internal responses designed to enhance adversary paranoia, and degrade operations efficiency due to the imposition of new operations security or personal/political reliability controls. An adversary inwardly focused after a major loss to CCO action may be presumed to be less likely to retaliate or escalate externally.

Third party actions by allies, partners, industry asset owners, or commercial intelligence services may help avoid negative outcomes. The separation of the mechanism of perceived impact from CCO action will likely change the adversary calculus of reaction, especially where it depolarizes a strictly bilateral conflict and presents the adversary with a multilateral problem space. However, such partnering need not entirely rule out or even limit unilateral CCO actions, but merely inform the timing and manner in which these operations are conducted when considered within the larger framework of relationships facing a crisis. The benefits of third-party action may naturally emerge from well-coordinated CCO engagement where the equities of these additional players are taken into account, and especially where CCO fits as one element within a wider defensive and countering campaign leveraging all instruments of national power.

The requirement to consider CCO and their potential consequences in this manner is more than somewhat novel for analysts, academics, and policymakers alike. CCO actions are driven by technical and tactical factors that nonetheless may result in what are essentially strategic interactions. Such interactions have been reserved previously for only a select few national capabilities. This demands greater focus and attention to the operational art involved, in order to illuminate differing employment scenarios, estimate adversary reactions, and understand higher order effects stemming from events in the domain. Evaluation of these factors in the context of such cases offers utility for future operations planning, indications and warning analysis, as well as simulation and wargaming evaluation.

Escalation risks are neither absolute nor preordained outcomes, and are likely highly sensitive to specific tactical and operational conditions shaped by specific facts "on the wire." Decisionmakers must remain wary of the specific scenarios under which escalation may be more likely due to unique sensitivities and through previously recognized dynamics. Yet there almost certainly remains a robust engagement space within which CCO actions may be conducted in a manner that minimizes chances of error, misinterpretation, and subsequent escalation. However, there are likely hitherto unanticipated implications for strategic stability—even as it remains further likely that repeated interactions to reset conditions of security and insecurity will over time reduce the strategic weight of specific campaigns, as both sides become better accustomed to implicit grammar, and tacit boundaries, of what may be seen as reasonable actions to contest ongoing espionage and other hostile access to critical systems and networks.

REFERENCES

[1] Robert Chesney, Max Smeets, Joshua Rovner, Michael Warner, Jon R. Lindsay, Michael P. Fischerkeller, Richard J. Harknett, and Nina Kollars, "Policy Roundtable: Cyber Conflict as an Intelligence Contest," *Texas National Security Review* (September 2020). https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/

[2] U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority" (April 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

[3] Jon R. Lindsay. "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity*, Vol. 1, No. 1 (2015), pp. 53–67; Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, Vol. 24, No. 2 (2015), pp. 316–348; Brian M. Mazanec and Bradley Thayer, *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace* (Palgrave Macmillan, 2015); Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol. 26, No. 3 (2017), pp. 452–481; Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (2017), pp. 44–71; Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis*, Vol. 61, No. 3 (2017), pp. 381–393; Jon R. Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *The Power to Hurt: Coercion in Theory and in Practice*, edited by Kelly M. Greenhill and Peter J. P. Krause (Oxford University Press, 2018).

[4] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022).

[5] Patrick J. Malone, "Offense-Defense Balance in Cyberspace: A Proposed Model," Naval Postgraduate School (December 2012); Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (2013), pp. 365–404; P. W. Singer and Allan Friedman, "Cult of the Cyber Offensive," *Foreign Policy*, 15 January 2014; Martin R. Stytz and Sheila B. Banks, "Toward Attaining Cyber Dominance," *Strategic Studies Quarterly*, Vol. 8, No. 1 (2014), pp. 55–87; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3 (2016–2017), pp. 72–109.

[6] Elena Chachko, "Persistent Aggrandizement? Israel's Cyber Defense Architecture." Working Group on National Security, Technology, and Law. Hoover Institution, Stanford University. August 2020.

[7] Deborah Bodeau, Richard Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment," *Mitre* (November 2013).

[8] Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly*, Vol. 12 (2018), pp. 9–113; Max Smeets and Herbert S. Lin, "Offensive Cyber Capabilities: To What Ends?," in *10th International Conference on Cyber Conflict*, edited by T. Minárik, R. Jakschis, and L. Lindström (Tallinn, 2018); Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* (2020); Max Smeets and JD Work, "Operational Decision-Making for Cyber Operations: In Search of a Model," *Cyber Defense Review*, Vol. 5, No. 1 (2020).

[9] Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies* (2021); Perri Adams, Dave Aitel, George Perkovich, and JD Work, "Responsible Cyber Offense," *Lawfare*, 2 August 2021.

[10] Dag Henriksen, "Control of the Air," in *Routledge Handbook of Air Power*, edited by John Andreas Olsen (London: Routledge, 2018); Gregg Courand, Cindy O'Reilly, and James R. Payne, "Offensive Counter-Air Mission Planning," Air Force Systems Command (1984).

[11] JD Work, "Rapid Capabilities Generation and Prompt Effects in Offensive Cyber Operations," International Studies Association Annual Conference, Las Vegas, NV, April 2021.

[12] James R. Gosler, "Counterintelligence: Too Narrowly Practiced," in *Vaults, Mirrors, and Masks: Rediscovering US Counterintelligence*, edited by Jennifer E. Sims and Burton Gerber (Washington, DC: Georgetown University Press, 2008).

[13] Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics," *Journal of Cybersecurity*, Vol. 5, No. 1 (2019); Benjamin Jensen and Brandon Valeriano, "What Do We Know About Cyber Escalation? Observations from Simulations and Surveys," *Atlantic Council* (2019); Erica D. Borghard and

Shawn W. Lonergan, “Cyber Operations as Imperfect Tools of Escalation,” *Strategic Studies Quarterly*, Vol. 13, No. 3 (2019), pp. 122–145; Erica D. Lonergan, “The Cyber-Escalation Fallacy,” *Foreign Affairs*, 15 April 2022.

[14] Martin C. Libicki, “Crisis and Escalation in Cyberspace” (RAND, 2012).

[15] Michael Fischerkeller and Richard Harknett, “Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation,” Institute for Defense Analysis (2018); Paul M. Nakasone, “A Cyber Force for Persistent Operations,” *Joint Forces Quarterly* (First Quarter 2019); Michael P. Fischerkeller, “The Cyberspace Solarium Commission Report and Persistent Engagement,” *Lawfare*, 23 March 2020; Richard J. Harknett, “Progress Is the Promise in National Cybersecurity Strategy,” 23 March 2020; Michael Fischerkeller, “Fait Accompli and Persistent Engagement In Cyberspace,” *War on the Rocks*, 24 June 2020; Paul M. Nakasone and Michael Sulmeyer, “How to Compete in Cyberspace,” *Foreign Affairs*, Vol. 99, No. 5 (September/October 2020).

[16] Jason Healey, “Triggering the New Forever War, in Cyberspace,” *Cipher Brief*, 1 April 2018; Max W. E. Smeets and Herbert Lin, “A Strategic Assessment of the U.S. Cyber Command Vision,” in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Institution Press, 2018); Erica D. Borghard and Shawn W. Lonergan, “How to Dampen Escalation Risks as Cyber-Attack Rules Loosen,” *Defense One*, 10 September 2018; Nina Kollars and Jacquelyn Schneider, “Defending Forward: The 2018 Cyber Strategy Is Here,” *War on the Rocks*, 20 September 2018; Jason Healey, “The Implications of Persistent (and Permanent) Engagement in Cyberspace,” *Journal of Cybersecurity*, Vol. 5, No. 1. (2019); Jacquelyn G. Schneide, “Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy,” *Lawfare*, 10 May 2019; Rose McDermott, “Some Emotional Considerations in Cyber Conflict,” Vol. 4, No. 3 (2019), pp. 309–325; James N. Miller and Neal A. Pollard, “Persistent Engagement, Agreed Competition and Deterrence in Cyberspace,” *Lawfare*, 30 April 2019; Jason Healey and Stuart Caudill, “Success of Persistent Engagement in Cyberspace,” Strategic Studies Quarterly, Vol. 14, No. 1 (2020), pp. 9–15; Max Smeets, “US Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection,” *Intelligence and National Security*, Vol. 35, No. 3 (2020), pp. 444–453; Benjamin Jensen, “Layered Cyber Deterrence: A Strategy for Securing Connectivity in the 21st Century,” *Lawfare*, 11 March 2020; Christopher Whyte, “Beyond Tit-for-Tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online,” Vol. 5, No. 2 (2020), pp. 195–214.

[17] Brandon Valeriano, “ … Concern about escalation is not speculation, its a real issue that the CC/DOD continually dismisses with no plans on how to mitigate risk in this area … ” Twitter, 25 August 2020, https://twitter.com/drbvaler/status/1298315593523892227; Jaclyn Kerr and Alexander Campbell, et al., “Workshop Summary Strategic Competition in Cyberspace: Challenges and Implications,” Center for Global Security Research, Lawrence Livermore National Laboratory, Livermore, CA, 10–11 July 2019; Brandon Valeriano and Benjamin Jensen, “The Myth of the Cyber Offense: The Case for Cyber,” Cato Institute, 15 January 2019; Jason Healey, “US Cyber Command: ‘When Faced

with a Bully… Hit him Harder,'" Cipher Brief, 26 January 2018; Herb Lin and Max Smeets, "What Is Absent From the U.S. Cyber Command 'Vision,'" *Lawfare*, 3 May 2018.

[18] "Cyber Command also executed offensive cyber and information operations. Each featured thorough planning and risk assessments of escalation and other equities. Each was coordinated across the interagency." From statement of General Paul M. Nakasone, Commander United States Cyberspace Command, before the House Committee on Armed Services, Subcommittee on Intelligence and Emerging Threats and Capabilities, 4 March 2020.

[19] Michael Martelle, "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War against ISIL," National Security Archive, 13 August 2018; Michael Martelle, "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY," National Security Archive, 21 January 2020.

[20] Len Anderson, Michael Martelle, Trey Herr, Audrey Alexander, Nina Kollars, and Pete Cooper, "Cyber Operations in Context: A Look at Joint Task Force Ares," Cyber Statecraft Initiative, Atlantic Council, 16 September 2019.

[21] Emily O Goldman and John Arquilla, "Cyber Analogies" (Naval Postgraduate School, 2014).

[22] Jason Healey, Neil Jenkins, and JD Work, "Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations," CYCON, Tallinn, Estonia, May 2020.

[23] Kurt Gottfried and Richard Ned Lebow, "Anti-Satellite Weapons: Weighing the Risks," *Daedalus*, Vol. 114, No. 2 (1985), pp. 147–170; Josephine Anne Stein, "Satellites, Anti-Satellite Weapons and Security," *RUSI Journal*, Vol. 133, No. 4 (1988), pp. 48–54; Charles F. Hermann, "Enhancing Crisis Stability: Correcting the Trend Toward Increasing Instability," in *New Issues in International Crisis Management*, edited by Gilbert R. Winham (New York: Routledge, 1988); Michael S. Gerson, "The Origins of Strategic Stability: The United States and the Threat of Surprise Attack," in *Strategic Stability: Contending Interpretations*, edited by Elbridge A. Colby and Michael S. Gerson (U.S. Army War College, Strategic Studies Institute, 2013).

[24] Matthew Mowthorpe, "The Soviet/Russian Antisatellite (ASAT) Programme during the Cold War and Beyond," *Journal of Slavic Military Studies*, Vol. 15, No. 1 (2002), pp. 17–28; Peter Vasilievich Zarubin, "Academician Basov, High-Power Lasers, and the Antimissile Defense Problem," *Optical Engineering*, Vol. 52, No. 2 (2013); Bart Hendrickx, "Naryad-V and the Soviet Anti-Satellite Fleet," *Space Chronicle*, Vol. 69 (2016).

[25] REN Ning and QIN Feng-ying, "Technique and Present State of Laser Countering Early-Warning Satellite, Electro-optics & Passive Countermeasures" (January 2003); XU Jun, WENG Xiaodong, and ZHOU Wenming, "Developments of American & Russian Laser Anti-Satellite Weapons," *Laser & Optronics Progress* (August 2003); MEI Guo-bao and Wu Shi-long, "Development, Application and Challenge Confronted with Electronic Reconnaissance Satellite," *Shipboard Electronic Warfare*, April 2005; Bates Gill and Martin Kleiber, "China's Space Odyssey—What the

Antisatellite Test Reveals about Decision-Making in Beijing," *Foreign Affairs* (May–June 2007); Gregory Kulacki and Jeffrey G. Lewis, "Understanding China's Antisatellite Test," *The Nonproliferation Review*, Vol. 15, No. 2 (2008), pp. 335–347; Michael P. Pillsbury, "An Assessment of China's Anti-Satellite and Space Warfare Programs, Policies and Doctrines," US-China Economic and Security Review Commission, January 2019.

[26] Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Crisis Stability in Cyberspace," Workshop on Cyber Escalation and Stability. *Texas National Security Review*, Vol. 86, No. 3 (29 May 2020).

[27] Karl Grindal, "Operation BUCKSHOT YANKEE," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healy (Cyber Conflict Studies Association, June 2013); Juan Andres Guerrero-Saade, Costin Raiu, Daniel Moore, and Thomas Rid, "Penquin's Moonlit Maze: The Dawn of Nation-State Digital Espionage," Kaspersky Labs and Kings College London, March 2018.

[28] Ankit Panda, "North Korean Hackers May Have Seen Secret US-South Korea War Plans," *The Diplomat*, 5 April 2017.

[29] Christopher Storrs, "Intelligence and the Formulation of Policy and Strategy in Early Modern Europe: The Spanish Monarchy in the Reign of Charles II (1665–1700)," *Intelligence and National Security*, Vol. 21, No. 4 (2006), pp. 493–519.

[30] James Stone, "Spies and Diplomats in Bismarck's Germany: Collaboration between Military Intelligence and the Foreign Office, 1871–1881," *Journal of Intelligence History*, Vol. 13, No. 1 (2014), pp. 22–40.

[31] Tim Mauer, "Solar Sunrise: Cyber Attack from Iraq?" in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healy (Cyber Conflict Studies Association, June 2013).

[32] Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: Harper, 2010); Matthew M. Aid, The Secret Sentry: The Untold Story of the National Security Agency (New York: Bloomsbury Press, 2009); Colin B. Burke, "It Wasn't All Magic: The Early Struggle to Automate Cryptanalysis, 1930s–1960," *United States Cryptologic History, Volume 6* (Center for Cryptologic History, National Security Agency, 2002), DECLASSIFIED; David A. Hatch and Robert Louis Benson, "The Korean War: The SIGINT Background" (Center for Cryptologic History, National Security Agency, 2000); Thomas R. Johnson, "American Cryptology during the Cold War, 1945–1989; Book I: The Struggle for Centralization, 1945–1960," *United States Cryptologic History Series, Volume 5*. Center for Cryptologic History, National Security Agency (1995). DECLASSIFIED.

[33] Marcin Siedlarz and Kristen Dennesen, "Hide and Seek: How Threat Actors Respond in the Face of Public Exposure," RSA Conference, Singapore, 20–22 July 2016.

[34] Department of Justice, "Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices," 23 May 2018; Cisco TALSO, "New VPNFilter Malware Targets at Least 500K Networking Devices Worldwide," 23 May 2018;

Symantec, "VPNFilter: New Router Malware with Destructive Capabilities," 23 May 2018.

[35] CISA, "New Sandworm Malware Cyclops Blink Replaces VPNFilter," 23 February 2022; National CyberSecurity Center, "Cyclops Blink Malware Analysis Report," 23 February 2022.

[36] Michael Warner, "The Kaiser Sows Destruction," *Studies in Intelligence*, Vol. 45, No. 1 (2002). UNCLASSIFIED.

[37] Thomas Boghardt, *Spies of the Kaiser: German Covert Operations in Great Britain during the First World War Era* (Springer, 2004), p. 118.

[38] Paul McMahon, "British Spies and Irish Rebels: British Intelligence and Ireland, 1916–1945" (Boydell Press, 2008), p. 357.

[39] Tom Clancy, *Red Storm Rising* (New York: GP Putnam, 1986).

[40] David C. Isby, "The Better Hammer: Soviet Special Operations Forces and Tactics in Afghanistan 1979–86," *Strategic Studies*, Vol. 10, No. 1 (1986), pp. 69–103; Egor Evsikov, "Soviet Intelligence in Afghanistan: The Only Efficient Tool of the Airmobile Troops and Soviet Airland War: From Afghanistan to the Future Politburo," *Baltic Security & Defence Review*, Vol. 11 (2009), pp. 41–57.

[41] Christopher Marsh, "Russian Risk, Hybrid Warfare, and the Gray Zone," in *Risk: SOF Case Studies*, edited by Bernd Horn (Canadian Special Operations Forces Command, 2020); Sergey Sukhankin, "Unleashing the PMCs and Irregulars in Ukraine: Crimea and Donbas," in *War by Other Means: Russia's Use of Private Military Contractors at Home and Abroad* (Jamestown Foundation, September 2019); Mark Galeotti. "Hybrid, Ambiguous, and Non-Linear? How New is Russia's 'New Way of War'?" *Small Wars & Insurgencies*, Vol. 27, No. 2 (2016), 282–301.

[42] Alex Kokcharov and John Raines, "Russia Begins 'Blitzkrieg' Invasion of Ukraine with Objective of Quick Victory; Intensive Fighting Likely across Country," *Jane's Intelligence Weekly*, 25 February 2022; Alex Kokcharov, "Kremlin's Potential Objectives and Limitations of Invasion of Ukraine," *Jane's Intelligence Weekly*, 28 February 2022.

[43] FireEye, "TEMP.Katar Expands Cyber Espionage Operations," 21 May 2016; Cymmetria, "Unveiling Patchwork—The Copy-Paste APT," July 2016; Andy Settle, Nicholas Griffin, and Abel Toro, "Monsoon—Analysis of an APT Campaign," *ForcePoint* (August 2016); Daniel Lunghi, Jaromir Horejsi, and Cedric Pernet, "Untangling the Patchwork Cyberespionage Group," *Trend Micro*, 11 December 2017; Brandon Levene, Josh Grunzweig, and Brittany Barbehenn, "Patchwork Continues to Deliver BADNEWS to the Indian Subcontinent, Palo Alto Networks, 7 March 2018.

[44] Ellen Nakashima, "Hackers Breach some White House Computers," *Washington Post*, 28 October 2014; Michael S. Schmidt and David E. Sanger, "Russian Hackers Read Obama's Unclassified Emails, Officials Say," *New York Times*, 25 April 2015.

[45] Malware sample ea3dd70963af5064e0431f86ca06cab6. Metadata dated 28 April 2017, https://www.hybrid-analysis.com/sample/583ddb480b42d04c7a8f960d950c7d52b46ed840354ae5cfa44d3c49e5239cab?environmentId=100; Anthony Kasza

and Micah Yates, “The Blockbuster Sequel,” Palo Alto Networks, 7 April 2017; Cyber Conflict Documentation Project, “JUCHE PHOENIX: Considering Potential DPRK Destructive Campaigns against US Critical Infrastructure Networks” (October 2017).

[46] Huib Modderkolk, “Dutch Agencies Provide Crucial Intel about Russia’s Interference in US-Elections,” 25 January 2018.

[47] ESET, “Sharpening the Machete,” 5 August 2019; Veronica Valeros, Maria Rigaki, Kamila Babayeva, and Sebastian García, “A Study of Machete Cyber Espionage Operations in Latin America,” *Virus Bulletin*, London, 2–4 October 2019; Blackberry Cylance, “El Machete’s Malware Attacks Cut Through LATAM,” 22 March 2017; Kaspersky, “El Machete,” 20 August 2014; Kaspersky Labs, “Unveiling ‘Careto’—The Masked APT,” February 2014; Kim Zetter, “Sophisticated Spy Tool ‘The Mask’ Rages Undetected for 7 Years,” *Wired* (10 February 2014).

[48] Dragos, “PIPEDREAM: CHERNOVITE’S EMERGING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS,” 13 April 2022; Mandiant, “INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems,” 13 April 2022; Cybersecurity and Infrastructure Security Agency, “APT Cyber Tools Targeting ICS/SCADA Devices,” 13 April 2022.

[49] Andy Bochman, Bryson Bort, Danielle Jablanski, Megan Samford, and Blake Sobczak, “PIPEDREAM at the Disco: Implications for International Security and Operational Technology,” Cyberstatecraft Initiative, Atlantic Council, 22 April 2022.

[50] Andy Greenberg, “A Mystery Agent Is Doxing Iran’s Hackers and Dumping Their Code,” *Wired*, 18 April 2019; Zach Dorfman, Kim Zetter, Jenna McLaughlin, and Sean D. Naylor, “Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks,” 15 July 2020.

[51] Sam Zeitlin, “Botnet Takedowns and the Fourth Amendment,” *New York University Law Review*, Vol. 90, No. 2 (2015), pp. 746–778.

[52] JD Work and Richard Harknett, “Troubled Vision: Understanding Recent Israeli–Iranian Offensive Cyber Exchanges,” Cyber Statecraft Initiative, Atlantic Council, July 2020.

[53] Proofpoint, “Not Dead Yet: Dridex Actors Resume Operation with New Distribution and Shifu Banking Trojan,” 30 October 2015; Brett Stone-Gross, “Dridex (Bugat v5) Botnet Takeover Operation,” *Secureworks*, 13 October 2015; U.S. Department of Treasury, “Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group behind Dridex Malware,” 5 December 2019.

[54] JD Work, “Who Hath Measured the (Proving) Ground: Variation in Offensive Capabilities Test and Evaluation,” 15th International Conference on Cyber Warfare and Security, Norfolk, VA, May 2020.

[55] Perri Adams, Dave Aitel, George Perkovich, and JD Work, “Responsible Cyber Offense,” *Lawfare*, 2 August 2021, https://www.lawfareblog.com/responsible-cyber-offense ; JD Work, “Balancing on the Rail—Considering Responsibility and Restraint in the July 2021 Iran Railways Incident,”

Offensive Cyber Working Group (UK), 23 September 2021, https://offensivecyber.org/2021/09/23/balancing-on-the-rail/

[56] David C. Gompert and Martin Libicki, "Waging Cyber War the American Way," *Survival*, Vol. 57, No. 7 (2015), pp. 7–28; Ben Buchanan, "Nobody But Us: The Rise and Fall of the Golden Age of Signals Intelligence," Aegis Series Paper No. 1708. Working Group on National Security, Technology, and Law; Hoover Institution, Stanford University. August 2017; Matthias Schulze, "Analysis of the Deterrent Potential of the New US Cyber Doctrine and Lessons for Germany's 'Active Cyber Defence,'" Stiftung Wissenschaft und Politik, August 2019; JD Work, "The American Way of Cyber Warfare and the Case of ISIS," *New Atlanticist*, 17 September 2019.

[57] Geronimo F. Nuno, "Chateau Cyber: Applying Historical Events to Military Innovation in the Cyber Domain," 13th International Conference on Cyber Warfare and Security, Washington, DC, 8–9 March 2018.

[58] Milan Vego, "Clausewitz's Schwerpunkt: Mistranslated from German—Misunderstood in English," *Military Review* (January–February 2007), pp. 101–109; John Robb, "The Systempunkt," *Global Guerrillas*, 19 December 2004.

[59] Lester Godefrey, "Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests," *Studies in Intelligence*, Vol. 66, No. 11 (2022).