JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 3(1), 2017, 69–80
doi: 10.1093/cybsec/tyx003
Advance Access Publication Date: 28 February 2017
Research paper

Research paper

Rules of engagement for cyberspace operations: a view from the USA

C. Robert Kehler, Herbert Lin* and Michael Sulmeyer

*Corresponding author. E-mail: herblin@stanford.edu

Received 2 February 2017; accepted 2 February 2017

Abstract

Cyber weapons provide US forces with operational choices that were previously unavailable. To use these weapons with greatest effect, the US military seeks to integrate them into its operational toolkit within a common framework of principles that apply to all weapons. While the US military has had decades of operational experience formulating rules of engagement (ROEs) for kinetic weapons, several characteristics of operations in cyberspace complicate the formulation of cyber-specific ROEs. Sensitive issues related to command and control and escalation of force play important roles in shaping cyber-specific ROEs. The article's conclusion is that a paucity of similar experience with cyber operations will hamper the formulation of ROEs for cyber weapons unless special efforts are taken to impart such experience to civilian leaders and military commanders.

Key words: cyberspace; cyber weapons; strategy

Introduction

As cyber weapons are incorporated into US military planning, policy makers and field commanders will increasingly confront a core issue: how to formulate the rules of engagement (ROEs) for US forces with regard to military operations that may use such weapons.[1] This article addresses ROEs from the perspective of US military operators.[2] It is informed by practitioner experience rather than empirical research.

The US Department of Defense (DOD) defines ROEs as "directives issued by competent military authority that delineate the circumstances and limitations under which US forces will initiate and/or continue combat engagement with other forces encountered" [2]. ROEs also provide authorization for and place limits on the use of weapons, the positioning and posturing of military forces, and the use or nonuse of certain specified capabilities (e.g. specific weapons systems). However, they are not generally used to assign missions or to give tactical instructions.

Understanding ROEs[3]

US military commanders act within a complex network of authorities derived from law, policy, and regulation. Authorities provide commanders with the permissions needed to conduct military operations. Such authorities include the authority to use force, of which ROEs are one critical component.

ROEs reflect constraints on the use of force imposed by the law of armed conflict (LOAC). These constraints include "military necessity," which permits only acts of force necessary to accomplish legitimate military objectives; "distinction," which distinguishes between combatants and civilians; and "proportionality," which counsels that the anticipated loss of life or injury to civilians or damage to civilian objects not be in excess of military advantages anticipated from a specific act.

In addition, senior leaders may wish for policy reasons to impose constraints that go beyond LOAC requirements. For example, they

1 In this article, cyber "weapons" and "capabilities" are used interchangeably for readability, even though not all cyber capabilities constitute cyber weapons.

2 Coalition activities whereby the USA conducts operations with allies and partners would be informed by this analysis, at least in part. Under some circumstances, US military forces also develop rules of engagement with local law enforcement as well. For example, the US Army and Marine's Counterinsurgency Manual notes that "[t]o work effectively together, the police and military coordinate rules of engagement" [1].

3 This section summarizes Appendix A, which is a primer on ROEs and related concepts, which will provide the foundation for understanding for the development of cyber-specific ROEs.

may wish to influence world opinion, to not antagonize an adversary unnecessarily, to conform to host country law, or to not escalate a conflict. Commanders may use ROEs to place upper bounds on the scope and intensity of operations to reduce the chances of undesired conflict escalation.

US forces operate under three types of ROE. Standing rules of engagement (SROE) provide a general set of always-operative rules related to self-defense for forces in peacetime as well as a template for operation-specific ROEs. Supplemental ROEs (also known as mission-specific ROEs) are tailored for a region, a mission, or a specific operation, and may elaborate on and/or interpret the SROEs for a given mission without contradicting them. Standing rules for the use of force (SRUF) govern military actions inside the USA.

SROE

The SROEs empower commanders at all levels to protect their forces from hostile acts and demonstrations of hostile intent. Unit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent, whether or not a state of armed conflict is acknowledged to exist.

The SROEs allow a US commander to use all necessary means available and to take all appropriate actions in self-defense, provided these actions do not violate the LOAC requirements of necessity and proportionality. However, they allow only those immediate actions minimally required (with respect to nature, duration, and scope of force) to end the immediate threat. Some weapons and tactics require specific approval from the President or Secretary of Defense before they can be used (e.g. only the President can authorize the use of nuclear weapons).

Self-defense includes passive and active defense measures. Passive defense refers to actions taken to "reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative," whereas active defense refers to the "employment of limited offensive action and counterattacks to deny a contested area or position to the enemy" [3].

In practice, the on-scene commander must make judgments about what constitutes hostile intent, a difficult task in a fluid and fast-moving tactical situation. Commanders are asked to use their best judgment when considering available intelligence, political and military factors, indications and warnings, and other relevant information concerning possible threats in their area. But there is no checklist of indicators that will conclusively determine hostile intent. Proactive measures (e.g. issuing warnings, firing warning shots) are encouraged if practical because entities that do not alter their behavior as a result are regarded as more likely to be showing hostile intent.

Supplemental ROEs

Supplemental ROEs are mission-specific and do not restrict the appropriate use of force in self-defense. Supplemental ROEs may be used to elaborate on how the SROEs should be interpreted in situations likely to occur during a specific mission. For example, a given mission might call for deployed forces to interact with civilians. If such interactions are unfriendly (e.g. an encounter with an unarmed mob), the risk of escalating a conflict may be high, and so a supplemental ROE might direct that the unit should withdraw or use smoke to camouflage itself, but should not use its weapons to fire on the mob.

Some supplemental ROEs permit a specific tactic, weapon, or operation. Others clarify action allowed under the SROEs. For example, they may limit specific types of artillery, who may use certain weapons, or the targets that may be attacked.

Because they are mission-specific, supplemental ROEs are an important focus of mission planning – a process that defines specific objectives, establishes lists of targets to be attacked to achieve those objectives, and develops courses of action and options for attacking each target. Mission planning is usually done well in advance of actual military action, but the existence of a mission plan does not have operational significance until commanders are given the authority to execute that mission. In contrast, the SROEs are always in effect and thus always have operational significance.

SRUFs

SRUFs govern military action inside US territory. Such actions can include those associated with Defense Support to Civil Authorities, land homeland defense missions, and law enforcement/security measures at DOD installations. SRUFs are inherently restrictive: unless specific weapons and tactics are explicitly approved, they cannot be used without the authorization of the Secretary of Defense.

Defense Support to Civil Authorities during Hurricane Katrina offers one SRUF example. In that mission, SRUFs were used to help guide the actions of conventional forces from the Navy, Air Force, and Army that were assigned to support civilian authorities with search and rescue, aid delivery, and peacekeeping.

Rules of engagement for cyberspace operations

ROEs for cyberspace operations have received growing attention as opportunities for achieving military objectives in and through cyberspace have become more plausible. To the extent feasible, the DOD has sought to apply the same principles that govern the use of kinetic weapons to the use of cyber weapons, while recognizing the special characteristics of the cyber domain and cyber weapons. This has proven to be a difficult challenge.

Many of the military's actual capabilities in the cyberspace domain and the ROEs corresponding to their use remain classified. That said, through inference, informed speculation, and an increasing public understanding of the underlying science and technology, a growing body of unclassified information is available regarding the principles and concepts that guide how DOD planners formulate ROEs for operations in cyberspace.

The meaning of self-defense

The SROEs are based on an immediate threat (i.e. the commander must determine that a hostile act has occurred or that hostile intent exists) and a need to respond to that threat. But an action that comes in or through cyberspace may not present an obvious threat to human life or critical capability. Rarely will a cyberspace operator confront a personal life or death decision similar to that of a solider engaged in kinetic combat on a physical battlefield,[4] meaning that cyberspace adds a new layer of complexity to the traditional concepts of self-defense.

The response to this new complexity has been a compromise. Military units are generally authorized to take passive defense measures within the systems or networks for which they are responsible. Examples include using intrusion detection systems (IDS – software that monitors the network or system for malicious activities), using firewalls that prevent traffic from passing through various ports or

4 This article uses "kinetic" as an approximate synonym for "non-cyber" or "conventional."

signature-based antivirus systems that screen incoming traffic for embedded malware, dropping connections that could be used for hostile purposes, or deleting malware found on the systems being defended. Such measures are analogous to evasive maneuvers for a ship facing an airplane that is apparently attacking.

On the other hand, a military unit experiencing a cyberattack would not be allowed on its own authority to conduct a cyberattack (or kinetic attack, for that matter) against the Ministry of Defense headquarters of the nation believed to be responsible. Such a response would be an overtly offensive action analogous to striking the airfield from which an attacking airplane was launched and would require separate authority.

Active defense occupies a large and uncharted grey area between passive defense and overtly offensive action. For all practical purposes, active defense can be defined as anything that is neither passive defense nor offensive action. As with all US military operations, active defense measures must comply with the laws of war regarding distinction, proportionality, and the like. In addition, active defense must not go beyond measures that negate or mitigate the immediate threat to the defender. In the cyber context, active defense is complicated by several unique factors.

Active defense measures in cyberspace can fall into two categories – those that have effects on systems or networks inside the organizational span of control of the defender, and those that have effects on systems or networks outside that span of control.[5] Active defense measures in the first category (Category 1) can include hunting within one's own network for malware, operating honeypots that attract adversary traffic, dynamically restricting privileges for suspicious users identified by an intrusion detection system, and so on. Such actions have few, if any, international legal implications. Category 1 active defense measures are analogous to launching intercept aircraft in response to an intruding enemy aircraft with orders to engage within the defender's airspace.

Active defense measures in the second category (Category 2) are much more problematic from an international legal standpoint because they do have effects on or require access to systems or networks not under the defender's legitimate control. Category 2 active defense measures could include disabling the computer controlling the hostile action or beaconing (the practice of "bugging" files so that they report when the adversary opens them). Category 2 active defense measures are analogous to an airplane flying in its own airspace that is illuminated by a fire-control radar located in an adjacent country and firing an anti-radiation missile at the radar. In all cases, differentiating between Category 2 active defense and offensive action in cyberspace can be problematic.

Cyber-related self-defense takes another turn when considering responses with noncyber means. Indeed, the DOD Cyber Strategy explicitly notes that the USA will "respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power . . . ." [4].

Thus, if the cyberattack originates from a nearby location, a unit might fire a missile to physically destroy the source of the attack. While a kinetic response is not symmetrical to the incoming cyberattack, there is no prima facie reason why it could not be proportional. However, such a kinetic response could be escalatory, and such escalation might be of significant concern to higher headquarters. Anticipating such a situation, higher authority might formulate restrictive ROEs on the unit so that explicit authorization is needed before responding in such a manner.

In addition, the effects of an active defense action are supposed to be limited to eliminating the immediate threat. Thus, any Category 2 active defense measure must employ weapons and techniques (cyber or otherwise) that confine damage to the threat entity and minimize damage to other systems. But as discussed in another paper in this volume [5], such a task places great demands on intelligence. A great deal of detailed intelligence information about the target of a Category 2 active defense action is needed to limit effects to the threat entity. Such information may not be available in a timely way.

To a certain extent, development of ROEs will inform intelligence gathering efforts about the possible targets, and therefore shape what entities may be targeted for Category 2 active defense.

Another problematic scenario involves a tactical unit using a cyberattack as a response to incoming kinetic fire – the responsive cyberattack launched in self-defense would target the computers powering the opponent's equipment. With just these facts, such a cyber-response might or might not be escalatory. Nor is it clear that such a response would be any more (or less) narrowly tailored than a kinetic response. If the cyber response knocks out the firing weapon but also regional internet traffic that connects civilian infrastructure, it is not clear if the cyber option is any better or worse than the noncyber options. These scenarios present important wrinkles to be considered when commanders prepare ROEs pertaining to self-defense in cyberspace.

Commanders typically prefer permissive (and clear) ROEs for military operations. Allowing units to respond with a range of capabilities (regardless of whether they are cyber or noncyber) with permissive ROEs that are sensitive to the unique aspects of cyberspace is arguably the most efficient method to shape how units react. But from a policy maker's perspective, the risks of inadvertent escalation and collateral damage may well argue for restrictive rules, especially when considering responses with noncyber means.

A final point on self-defense – the more individualized notion of unit self-defense must be distinguished from the broader concept of defending the country, its interests, or its property [6]. Self-defense in the latter case is functionally distinct from the type of self-defense envisioned in the SROEs. Separate authorities (i.e. supplemental ROEs) would have to be crafted to cover cyber actions taken in conjunction with DOD actions to defend the nation, or SRUFs would have to be developed to cover DSCA activities.

In general, active defense measures and deadly force through cyberspace could be authorized to protect people or capabilities that, if damaged or destroyed, would reasonably threaten death or serious bodily injury. Deadly force could not be used to defend most kinds of property, although generally passive defense measures can be taken (move the property, house it, lock it up, build a fence around it, and so on). However, according to Joint Chiefs of Staff instruction CJCSI-3121-01B, Enclosure L (SRUF) [7], certain special categories of property can be protected with deadly force. These include:

- Assets vital to national security, such as nuclear weapons, nuclear command and control, designated restricted areas containing strategic operational assets, sensitive codes or special access programs.
- Inherently dangerous property, such as portable missiles, rockets, arms, ammunition, explosives, chemical agents, and special nuclear materials.
- National critical infrastructure, which include presidentially-designated public utilities or similar critical infrastructure, vital

5 Note that these categories are not terms recognized in U.S. military doctrine or literature – they are introduced here only for ease of exposition in this article.

to public health or safety, the damage to which would create an imminent threat of death or serious bodily harm.

Given that deadly force is authorized to protect the above kinds of property, it is likely that the use of cyber weapons for the same purpose would be allowable under the SRUF. But the considerations described below may well weigh against such use in many circumstances.

Ambiguous intent

"Hostile intent," i.e., the imminent use of or threat of force, is a foundational concept on which the SROEs are built [8]. However, in the cyber domain, determining the intent behind network activity can be confounding. For example, differentiating between enemy reconnaissance in cyberspace and enemy preparation for an imminent attack is very difficult, as both operations entail essentially the same activities from a technical perspective. Distinguishing between reconnaissance and routine intelligence collection is even more problematic. The majority of adversary objectives in cyberspace have heretofore been to create access to systems and data, to maintain persistent presence on those systems, and to steal information and intellectual property. Thus, distinguishing hostile intent from these other activities is a challenge for operators trying to apply ROEs in a timely way.

As an example, an attempted intrusion against an important military facility may be motivated by the desire to collect information without tactical military value. Such intent, though certainly not friendly, most likely does not rise either to the level of a hostile act or to the demonstration of hostile intent. But the intrusion may also be the precursor to a cyberattack that will cause actual damage, which would be a hostile act. When the intrusion is detected, it may not be entirely clear which of these possibilities is the case, and a delayed response may be too late.

The lack of clarity arises from an inherent characteristic of cyber instruments. Such instruments require a mechanism to penetrate the system of interest and a separate mechanism (usually called the payload) to create the desired effects. When the intrusion is first detected, the payload may not have yet executed, making determination of the intrusion's purpose difficult.

A second example is that of port scanning, an action that determines which ports are open at a given IP address. An IP address specifies the location of a specific computer system in cyberspace at a specific time, and ports are channels through which that computer can transmit and receive information. Specific ports are often but not always associated with certain functions – Port A is used for passing information to and from the World Wide Web, Port B is used for email, and so on. The system administrator can open or shut down ports depending on the needs of the system's user – but often ports that are left open unnecessarily are used by intruders to gain access to the system.

Should port scanning of a military facility's computer system be regarded as a hostile act in the meaning of the SROE, even if nothing happens as the result of that scan? According to then-Rear Admiral Betsy Hight of the Joint Task Force on Global Network Operations as reported in a 2009 report of the National Research Council [9], an action that resulted only in inconvenience to the probed unit or that appeared directed at intelligence gathering did not rise to the threshold of warranting an active defense measure.

Ambiguity of intent need not preclude active defense responses, especially those in Category 1. Even if it were possible to definitively prove a penetration had purely defensive (and therefore nonhostile) purposes, network defenders would still carry out all possible responses to remove it, given the risk of future exploitation or hostile action. Furthermore, passive and Category 1 active responses are aimed at eliminating the threat without undertaking any activity outside of the defender's network. If, for example, malware is found on a given computer and has not spread, disconnecting that computer from the network eliminates the threat without regard for an intruder's intent.

ROEs may therefore need to make greater accommodation for the ignorance of intent when defining when and under what conditions cyberspace operators may act, especially when compared to rules for kinetic operations.[6] Alternatively, the standard of evidence required to determine intent may need to be lower than kinetic operations.

Finally, resolving ambiguity is compounded by a definitional problem. When every bad thing happening is characterized as a cyber "attack," it is far more difficult to characterize anything as a real attack. Clarity in this definition is an important precursor to understanding intent.

The (putative) need for speed in the meaning of self-defense

In the kinetic world, reacting quickly is often necessary to eliminate an immediate threat. For example, illuminating an aircraft with a fire-control radar often indicates that a missile is about to be launched against it, and delaying the destruction of that radar is likely to increase the likelihood that the aircraft will be attacked and destroyed.

Similar considerations have been applied to threats in cyberspace. Given the speed with which a cyber threat may cause harm, a response action may be needed very quickly to eliminate or disrupt it. In fact, the time scale on which action is needed may be so short as to preclude human intervention. However, automated response may lead to unintended and collateral effects for which the consequences are not fully understood.

Consequently, cyber ROEs must account for some likely combination of enhanced machine-based indications and warning, careful automated responses, and human decision-making. In 2007, the USAF sought proposals for a Cyber Control System to support automated active defense operations [10]. Today, policy makers are wary of demands for speedy (and thus automated) responses, concerned about machine-driven escalation.

Command and control

In a traditional kinetic attack, conventional US military forces generally possess some resources that they can use in self-defense. For example, ground combat units likely carry weapons that they can use to target and silence the source of incoming fire. In cyberspace operations, however, a unit subject to cyberattack may not have all the resources needed to respond effectively. For example, consider network administrators at US Pacific Command (PACOM) who see their unclassified networks subjected to a denial of service attack. These individuals may have to rely on both internal and external

6 An approximate analog from kinetic operations might be a scenario in which soldiers are involved in urban combat where armed civilians and insurgents are intermingled. ROEs in this scenario might specify that soldiers are authorized to fire their weapons when – and only when – fire is being directed at them rather than when fire is occurring without singling them out as specific targets. This example is inspired by the film *Blackhawk Down*.

sources of support, all of whom may be operating under separate authorities and ROEs.

Headquarters staff will be required to draft cyber ROEs with full awareness of evolving cyberspace command and control arrangements. According to a 2011 document, command and control structures may differ depending on combatant commander authority, operational control, tactical control, administrative control, supporting, and direct support relationships [11].

Borderless geography and range of effects

Internet routing protocols route data by and through routers according to a series of rules that seldom include distinctions based on geopolitical boundaries. This reality has two consequences. First, it is almost impossible to route traffic on the Internet in a way that is confined to physical-world geographies. This factor makes it difficult (though not necessarily impossible) to contemplate cyber operations, whose planning necessarily includes routing considerations, that are wholly confined to a specific geographic area. Second, the same reality also enables adversaries to exploit compromised infrastructure both inside and outside of the USA to attack US networks.

Because hostile acts in cyberspace may cross national boundaries, the physical distance between where the attack originates and where it has its effects may be large. The same is true for any defensive response action, whose range may be similarly large, and a cyber response action may create effects thousands of miles away. This situation would be analogous to one in which a surface-to-air missile fired against an attacking airplane could have destructive effects on a city on the border of a neutral third country into which the airplane crashes, although in reality both an attacking airplane and a surface-to-air missile fired against it in defense of a ship have comparatively limited ranges.

Cyberspace ROEs must account for these geographic realities of cyberspace. This may call for blending the SROEs and their homeland counterpart, the SRUF. Arrangements between DOD and the Federal Bureau of Investigation and other relevant domestic agencies will be needed for situations when cyber activity implicates their jurisdiction. A coalition or alliance approach to creating ROEs may also be needed that acknowledges the potential of cyber operations to occur and create effects in multiple international political jurisdictions.

Pre-kinetic military operations in anticipatory self-defense

The DOD Cyber Strategy released in April 2015 states explicitly that "[d]uring heightened tensions or outright hostilities, DOD must be able to provide the President with a wide range of options for managing conflict escalation" [12]. By definition, periods of heightened tension occur prior to the outbreak of outright hostilities, and thus this statement suggests that offensive cyber operations may well "precede" kinetic operations.[7]

The USA takes the position that nations have "the right to take measures in response to imminent attacks."[8] An imminent attack is one that has not happened yet (i.e. the first damage from such an attack has not yet been suffered) but rather is about to happen, and the USA – as do many other nations – reserves the customary international law right of anticipatory self-defense. (This right is contested in the academic literature as well as by nations that believe they have unjustly been the targets of such a response) [16].

An important question for anticipatory self-defense is the degree and nature of the evidence needed make the determination that an attack is imminent, but there is no consensus on answers for this question.[9] A determination of imminence could be based in part on information provided by human intelligence (e.g. an informant embedded with an adversary), technical intelligence (e.g. photos showing the massing of military forces in critical areas), or signals intelligence (e.g. interceptions of adversary communications suggesting an imminent attack). In cyberspace, signals intelligence could include information derived from sensors that have been pre-positioned inside adversary networks.

However, once such a determination of imminence is made, SROEs relating to cyber operations may state that commanders are authorized to conduct such operations as part of an anticipatory self-defense effort. Other guidance or advice may or may not constrain how that determination of imminent attack is made, e.g., by reiterating to the commander the need for high confidence in the determination or giving him or her access to sources of intelligence that might not otherwise be made available.

Under this doctrine, exercising the right of anticipatory self-defense requires necessity and proportionality.[10] While meeting the necessity requirement is the threshold for acting in anticipatory self-defense, meeting the proportionality requirement is almost certainly easier using cyber operations that shut down adversary military capabilities rather than destroy them kinetically (e.g. by inhibiting adversary missile launches through cyberattacks against their launch facilities or their command and control systems).

Finally, operational preparation of the cyber battlefield (OPB) is likely to be an ongoing activity as routine as peacetime reconnaissance or surveillance of potential adversary activity. OPB involves an active search for vulnerabilities in and access paths to adversary systems and networks and when possible, implantation of "hooks" that will facilitate later overtly destructive cyber action should such action be necessary. The key characteristic of OPB is that it is not a destructive act in any way; even so, the scope and nature of OPB is

7 A good discussion of offensive operations in cyberspace as they relate to kinetic conflict, especially in times of crisis, can be found in [13].

8 See [14]. Also, in a 2015 article, DeWeese argues that anticipatory and preemptive self-defense "can be applied against imminent [cyber] threats in a similar manner to kinetic threats," but also that "putting a measure on how to determine imminence against threats in cyberspace presents challenges which States have not previously confronted from conventional threats" [15].

9 As noted by Gill and Ducheine [17], "the ICJ employed a stringent standard that rejected 'suggestive' and 'highly suggestive' evidence of Iranian involvement in attacks on international shipping in the Persian Gulf. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 59, 71 (Nov. 6). This and other aspects of the judgment were vigorously criticized by a number of judges in their individual opinions. See id., ¶¶ 30–39 (separate opinion of Judge Higgins); id., ¶¶ 21–30 (separate opinion of Judge Kooijmans); id., ¶¶ 33–46 (separate opinion of Judge Buergenthal); id., ¶¶ 33–40 (separate opinion of Judge Owada)."

10 In this context, proportionality is the requirement that the degree and kind of forceful response must not exceed that which is minimally needed to forestall the imminent attack. As such, this type of "jus ad bellum" proportionality is different from "jus in bello" proportionality in conducting attacks discussed earlier. See, e.g., [18] and [19].

likely to receive attention from higher authority because of its sensitivity and escalatory potential.

Forms of offensive operations in cyberspace

The US Cyber Mission Force may conduct two forms of operations that could be characterized as offensive. The first is the mission of "generating integrated cyberspace effects in support of operational plans and contingency operations" [20]. For example, in February 2016, Secretary of Defense Ash Carter described how cyber operations are supporting the broader campaign against the Islamic State in Iraq and the Levant [21]. This form of offensive cyberspace operation may be seen as supporting or enabling other, probably kinetic, activities.

US Cyber Command is also charged with defending the nation from a cyberattack of significant consequence. Just how they are to accomplish this mission is not publicly discussed at great length, but the DOD strategy document and other statements imply action beyond blocking and after-action mitigation [22]. Furthermore, the document's implementation objectives for the defend-the-nation mission refer multiple times to the need to deter cyberattacks of significant consequence. Though the deterrence by denial has a relationship to more defensive-type actions, deterrence by cost imposition can imply more offensive steps. The implication for commanders is that both types of offensive missions may need to be accounted for in ROEs.

Escalation of force

In physical space, escalation of force (EOF) measures are a set of actions, taken in sequence, that begin with nonlethal force measures such as visual signals (e.g. flags, spotlights, lasers, and pyrotechnics) and may graduate to lethal measures (direct action) such as warning, disabling, or deadly shots to defeat a threat and protect the force [23]. EOF measures support ROE objectives by helping soldiers to evaluate whether an approaching threat presents hostile intent and to decide the appropriate level of response.

Even in traditional operations, the decision to escalate force is highly subjective to the commander under threat. But this subjectivity is compounded in cyberspace, where intent is harder to establish and certain individual acts may not be inherently more escalatory than others. To be sure, if a cyberattack wipes 30 000 hard drives[11] or causes physical destruction,[12] it would be higher on the ladder of escalation than a low-level denial of service attack. But which is most escalatory: opening a seemingly innocuous port, a request to a foreign server to retrieve data, injecting code to access a hidden database, or installing a root kit that enables administrator-level access on a compromised computer? Context will always shape the answer to this question, but ambiguities in escalation will complicate interpretations of ROEs.

As such, EOF measures will need to be adopted to account for the uncertain nature of escalation within cyberspace. One method to do so might be to distinguish activities using the confidentiality, integrity, and availability framework.[13] For example, it may be more important for a logistics support operation maintaining data availability over other objectives, whereas an intelligence operation may prioritize confidentiality instead. Compromises to lower priority objectives would be treated as lower levels on an escalation ladder.

Attribution

In the context of responding to a hostile act or a demonstration of hostile intent, determining the party responsible for an intrusion may be difficult. This is the well-known attribution problem in cyberspace. Certain passive defense actions, such as raising one's own defensive posture, are almost always appropriate because they do not cause harmful effects on systems without the permission of the owners of those systems. But causing harmful effects outside one's own systems or without permission on the systems of others has many implications, political and otherwise.

Attribution of a hostile act in cyberspace is often possible when analysts have time to draw on multiple sources of information, both historical and collected in the wake of the hostile act in question. Such time may not be available in a tactical situation involving a hostile act, which may play out in seconds or minutes. The information available under these circumstances is unlikely to support a high-quality attribution judgment, and time lines will be short. How these considerations are ultimately addressed in cyber ROEs is a key matter for consideration and resolution.

Reconciliation of ROEs and SRUF

As noted above, the SRUF govern behavior of US military forces within the USA while ROEs govern behavior outside US boundaries. But cyberspace – and operations within it – increasingly blurs the line between national and international boundaries. In such instances, the SRUFs and the SROEs would have to be reconciled or integrated.

As an example of a potentially problematic scenario, imagine a foreign nation that takes control of a computer within the USA and uses it to launch a cyberattack of significant consequence against the Pentagon. If the identity of the foreign nation is known with a high degree of confidence (a big if!), SROEs may allow a Category 2 active response against the computer originating the attack even if it is located in that country. But if not, it may be that the only active response possible would be against the computer in the USA, an action that would implicate SRUF.

Discussion

ROEs provide military forces with guidance from higher authority about when and under what circumstances they may take various kinds of actions without further orders. As such, they must be sufficiently clear to provide guidance in situations or circumstances that military forces are likely to encounter – tragedy may befall units that encounter situations not anticipated or that cannot be handled under their ROEs.

Accordingly, key terms such as "hostile act" and "demonstration of hostile intent" must have clear definitions. In the world of kinetic weapons, the understanding of how ROEs should be interpreted has evolved as practical experience has accumulated over a period of

11 In 2012 the Shamoon virus infected the computer network of Saudi Arabia's national gas company, Aramco. The attack rendered over 30 000 machines unusable by overwriting their master boot records. Shamoon is speculated to have been carried out by Iran, but this remains unproven [24].

12 For example, in 2007, the Idaho National Laboratory conducted the "Aurora" experiment highlighting vulnerabilities in the electrical sector. The experiment used a cyberattack to change the operating cycle of a generator, causing the generator to break down [25].

13 A description of the confidentiality, integrity, and availability framework (also known as the CIA triad) can be found in many places. See, e.g., [26].

many years. Experience has demonstrated that exceptional or unusual circumstances not anticipated in the interpretation of ROEs occur frequently. Commanders and military lawyers have accordingly learned more about such "edge" cases and have developed operationally useful interpretations based on these experiences, even as kinetic weapons evolved much more slowly.

In contrast, cyber weapons are relatively new, and most unit commanders have not had the opportunity to accumulate a comparable experience base in understanding how any given ROE might apply in cyberspace. Furthermore, many possible adversaries are acquiring offensive cyber capabilities, and their number is growing, increasing the urgency of developing such understanding. One approach for meeting this urgent need is to provide intensive experiential training for unit commanders in responding to scenarios that mimic as closely as possible the range of scenarios that they may encounter.

A second important point is that many of the problematic issues for interpreting the SROEs in cyberspace arise from Category 2 active defense actions. Active defense against kinetic weapons focus on negating the immediate threat, a fact with two implications. First, the immediate threat is generally near the entity being defended, and thus action taken against it need not affect anything else that may be farther away. Second, speedy negation is essential – because the threat is physically near the defended entity, there is only a short time available to eliminate it. In some situations involving kinetic weapons, an automated response may be necessary. For example, the Phalanx Close-In Weapon System (a radar-guided Gatling gun intended for defense against incoming supersonic cruise missiles) has a fully autonomous mode in which it will shoot automatically at any target meeting certain specified parameters (e.g. if a missile has a speed, range, and bearing that would put it on an intercept course toward the defended entity).

But cyber weapons are of a different character. The threatening cyber weapon is a software or hardware artifact that is physically located somewhere – either on the defender's own computer systems, the attacker's computer systems, or perhaps the computing infrastructure of a third party. Taking action against one's own systems (e.g. shutting down computers) is not problematic from a policy point of view, but taking action against an attacker's computer systems may be, as discussed above.

Additionally, one important reason – perhaps the most important reason – for having ROEs in the first place is to inhibit the unintended escalation of conflict. ROEs help to ensure that that US actions do not lead the military forces of a potential opponent to escalate into a "self-defense" response [27]. Actions that are considered and deliberate are less likely to result in unintended escalation than actions that are reflexive. Given the potential escalatory consequences of an automated response that has damaging or destructive effects on the attack-originating entity, rapid responses may not be desirable from a policy perspective.

Put differently, policy considerations may well dictate – or at least suggest – that Category 2 active defense actions, i.e., those that have damaging effects on systems outside the unit's organizational purview, should not be allowed under certain circumstances. Although emerging US military doctrine seeks to integrate cyber weapons into an effects-based framework that applies to all weapons, applying the requirement for speedy action in a Category 2 active defense response to a cyber threat – a requirement that may necessarily entail automated responses – may not serve US interests in reducing the likelihood of escalation.

A third issue is the actual utility of Category 2 active defense actions in negating cyber threats. Negating a cyber threat can only mean one of two things – preventing an initial threat from seriously affecting the unit's computer systems or preventing follow-on threats from doing so. If SROEs allow Category 2 active defense actions only when the threat rises to the level of impairing mission performance capabilities (as was true in 2007), it is highly likely that the damage will already have been done by the time it is possible to launch a response.

That leaves the possibility that a Category 2 active defense response might be able to disrupt the computer systems responsible for the original attack so that further attacks will not take place. But this scenario is for all practical purposes indistinguishable from taking overtly offensive action – and it has one added complication. After the initial attack, an informed adversary can simply take the originating computers offline to make them immune to any response, and others can be brought online from different locations in cyberspace should further attacks be needed.

Given that Category 2 active defense measures involving destructive or damaging action against adversary computers will require both rapid response and significant intelligence to be available, such measures are likely to be undesirable in many operational scenarios.

Conclusion and recommendations

The above discussion has suggested that when the principles guiding the formulation of ROEs for kinetic weapons are applied to cyber weapons, some ROE considerations are quite similar and others are considerably different. As commanders gain greater experience with cyber operations, how to interpret ROEs and indeed to formulate them will become clearer.

At the same time, ROEs in other domains have evolved over many years of operational experience. Because the potential significance of cyber operations, both defensive and offensive, is rapidly growing, the US military does not have the luxury of time to develop such experience for such operations. So an important policy issue today is how to help commanders (and planning staffs, including their Judge Advocate Generals) gain the experience that will help them use cyber weapons effectively – a key part of which is developing good ROEs for their use. In the past, the use of cyber weapons has been impeded more by legal and policy considerations than by the unavailability of the requisite technical or operational capabilities.

The authors of this article believe that tabletop exercises and war games with senior leaders and practitioners (including industry and commercial operators) are one way to help military commanders (and others in both the government and private sectors) gain experience necessary for formulating good ROEs for using cyber weapons. Such activities will force the participants to focus on definitions, boundaries, and the other issues that raised in this article. They will also force greater information sharing and help bridge the natural gaps between domains and sectors. Additionally, they will help familiarize commanders with realistic cyber options, what is possible to do with cyber, and most importantly, how they might wish to instruct their forces on the use of those options. As an example of such an exercise, it may be useful to develop ROEs and SRUFs appropriate for a distributed denial of service activity using compromised infrastructure both inside and outside of the USA.

To be useful, these exercises and games will require the personal involvement of the actual individuals that will be engaged in conflict. No serious military leader would expect soldiers to learn their combat craft primarily by reading reports of exercises involving others, and so the US military stresses a philosophy of units training as they expect to fight. There is no reason that cyber training should be any different.

Tabletop exercises and war games have the further advantage that they are framed around specific scenarios. No one scenario captures the full range of possibilities that commanders may face in combat, but commanders that participate in a number of exercises and games will be exposed to many more eventualities.

The authors expect that the most difficult scenarios for formulating appropriate ROEs are likely to be those involving active defense measures that may have effects on or that require access to systems or networks not under the defender's control (what were called Category 2 active defense measures above). The reason that active defense measures may be the most difficult is that they are likely to be at issue mostly during times that are not characterized by overt and acknowledged hostilities. During hostilities, of course, it is expected that military operations, both cyber and noncyber, may be taken that affect entities under the other side's control. Other scenarios may be less problematic, but that does not mean it will be easy to formulate ROEs for them. ROEs for cyber capabilities do present issues that are different in practice than those encountered, and until US commanders and their planning staffs are more familiar with operations in cyberspace, they will be unduly constrained in their combat roles.

Appendix A: A primer on rules of engagement

Military commanders and authority to act

US military commanders act within a complex network of authorities derived from law, policy, and regulation. Authorities provide commanders with the permissions needed to conduct military operations as well as forming the basis of domestic and international legitimacy for those operations.

The authority to use force is common to virtually every military operation; other authorities might include authority to organize forces to accomplish a mission, or authority to delegate operational or tactical control of those forces [28]. Typically, "the use of force is governed by international law (chiefly the principles of the Law of Armed Conflict), national law, national and coalition ROE (and Rules for the Use of Force in domestic operations), national caveats, and guidance and intent from superior commanders" [28]. ROEs make up one critical component of a commander's authority to use force. Commanders must understand and apply other sources of authority to establish context for those ROEs.

The scope and nature of ROEs

ROEs reflect three forms of influence:

- International over national: Principles of the LOAC are often incorporated in ROEs in ways that govern how national forces employ force, thus restraining a commander's actions so that they are conducted in a manner consistent with such law. As a matter of policy, sometimes the ROEs impose greater restraints on behavior than those required by international law, as indicated in the next item.
- Civilian over military: Motivated by considerations of policy and politics, civilian authorities such as the President of the USA and the Secretary of Defense issue ROEs to Combatant Commanders to govern the conduct of military operations, including the use of force.[14] That is, ROEs are part of ensuring that the actions of commanders in the field are consistent with national policies and objectives. For example, for various policy reasons such as a desire to influence world opinion, not unnecessarily antagonize an adversary, conform to host country law, or not escalate a conflict, national policy makers may issue ROEs that restrict the engagement of certain targets or forbid the use of particular weapons systems.
- Military over military: Combatant Commanders may issue ROEs to their component and/or subordinate commands from a perspective of tactics. These ROEs provide the parameters within which the commander must operate to accomplish the assigned mission. They place an upper bound on operations so that the commander's actions do result in undesired escalation of a conflict. They also grant or withhold the commander's authority to employ certain weapons or tactics.

The three types of influence described above are listed in order of specificity, with "international over national" being most general, and "military over military" being most specific.

ROEs for US forces are informed by principles of international law, such as: "military necessity," which permits only acts of force necessary to accomplish legitimate military objectives; "distinction," which distinguishes between combatants and civilians; and "proportionality," which counsels that the anticipated loss of life or injury to civilians or damage to civilian objects not be in excess of military advantages anticipated from a specific act. Among most modern states, these principles are uncontroversial. But how these principles of international law are interpreted in practice is the subject of much debate.

US forces operate under SROEs, which provide a general set of always-operative rules related to self-defense for forces in peacetime as well as a template for operation-specific ROEs [29]. SROEs are always operative, and impose limits on the actions of units in the field. Standing rules can be augmented by supplemental ROEs (also known as mission-specific ROEs), which can be tailored to a region, a mission, or a specific operation [30]. Supplemental ROEs may elaborate on and/or interpret the SROEs for a given mission, but supplemental rules should not contradict standing rules. Supplemental ROE can apply to specific operations (like cyberspace operations) and to the employment of specific types of weapons (like cyberspace capabilities) [31]. Finally, the SRUF govern US military actions inside the homeland.

Standing rules of engagement

The SROEs are issued by the uniformed Chairman of the Joint Chiefs of Staff and approved by the civilian Secretary of Defense [29]. The current version of the SROEs came into force on 13 June 2005 [29]. While much of that document is classified, the following discussion is derived from unclassified portions of the 2005 document, as well as its antecedent from 2000.

The SROEs provide "implementation guidance on the inherent right of self-defense and the application of force for mission accomplishment" [29]. The former give commanders authorities such that they always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent [32], whether or not a state of armed conflict is acknowledged to exist. The authorized means and methods of self-defense can also be limited based on concerns relating to the political environment, resources, and the like. For example, "Don't fire until you see the

14 A "Combatant Commander" is the commander of one of the unified or specified combatant commands. At present, the unified commands of the Department of Defense include US Africa Command, US Central Command, US European Command, US Northern Command, US Pacific Command, US Southern Command, US Special Operations Command, US Strategic Command, and US Transportation Command. There are no specified commands today.

whites of their eyes" would be a SROE limitation based on resource conservation. National leadership may limit the use of certain weapons in certain situations as well.

Under the SROEs, US forces may use all necessary means available and all appropriate actions in self-defense, as long as they are consistent with the LOAC requirements of necessity and proportionality. This interpretation is generally understood to mean taking action that is minimally required (with respect to nature, duration, and scope of force) to end the immediate threat. Note, however, that some weapons and tactics require specific approval from the President or Secretary of Defense before they can be used (e.g. only the President can authorize the use of nuclear weapons).

In practice, on-scene commanders must exercise good judgment in interpreting how ROEs apply in specific situations: while ROEs provide guidance and some limitations, they must avoid excessive constraints on forces operating in the field. This point is especially important when commanders are unable to communicate with higher authority in a timely fashion. Clarity and specificity are often sought by subordinate units, but breadth and generality are often provided at first to account for the broadest array of circumstances.

Ascertaining hostile intent is often difficult in a fluid and fast-moving tactical situation. Commanders are generally asked to use their best judgment when considering available intelligence, political and military factors, indications and warnings, and other relevant information concerning possible threats in the area of operations. However, there is no checklist of indicators that will conclusively determine hostile intent.[15]

Commanders are encouraged to use proactive measures, if practical, to determine the intent of an entity that poses a threat, such as issuing verbal warnings, sending visual or auditory signals, making use of physical barriers, changing course and speed to determine if the entity is continuing on an attack profile, illuminating the threat with fire control radar, or firing warning shots. Entities that do not alter their behavior are regarded as more likely to be showing hostile intent.

A canonical example of applying the SROEs would be a Navy ship under peacetime circumstances that observes an inbound airplane that may pose a threat.

- Under the SROE, the ship would always be allowed to take evasive action by maneuvering, to warn the airplane not to approach further, or to activate electronic countermeasures to jam the airplane's radar. (Such action would be regarded as "passive defense."[16]) These measures may eliminate the apparent threat. They are also nondestructive and as such do not escalate unnecessarily.
- Under the SROEs and depending on circumstances, the ship may be allowed to launch a surface-to-air missile to destroy the airplane. (Such action would be regarded as "active defense."[17]) For example, active defense may be appropriate only when passive defensive measures have failed.
- Under the SROE, the ship would not be authorized to launch a land-attack missile against the airbase from which the airplane was launched. (Such action would exceed that which is needed to eliminate the immediate threat and would constitute offensive action.) However, such a measure could be allowed under certain mission accomplishment ROEs or after obtaining higher-level approval for doing so.

ROEs – especially the SROE – tend to be more restrictive before the outbreak of hostilities. They are more open-ended during hostilities, and they return to being more restrictive after hostilities cease. Such transitions from less to more restrictive or vice versa do not necessarily reflect specific principles of international law, but rather the policy prerogatives of senior US leadership.

To illustrate, consider a developing crisis in which US military forces are initially dispatched as advisors with a specific mission to train and assist indigenous forces. These US forces would maintain their inherent right to self-defense, but the ROEs may limit their geographic movement, under what conditions they may open fire, or when different categories of personnel (civilian, combatant) may be detained [35]. If the mission for these US forces changes to reflect combat-related objectives, such as killing and capturing enemy combatants, the ROEs may relax limitations on geographic movement, on detention, or the types of weaponry that may be employed. When a specified area is cleared of combatants, US forces may be called upon to provide stability in the absence of functioning local governance. A less militarized presence may be desirable under these circumstances, and so the ROEs may again limit movement, detention, and munitions use.

Thus, ROEs may change as a conflict evolves. Such changes also entail an even greater level of complexity for subordinate units, as these units must interpret evolving ROEs from higher headquarters as the nature of a particular mission evolves. In this dynamic environment, supplemental ROEs are particularly important.

Supplemental ROEs

Supplemental ROE are mission-specific. They seek to further limit or enable distinct actions for mission accomplishment and require additional approval from higher authority. Supplemental ROEs pass these authorities to the relevant commanders.

There are two types of supplemental ROEs: permissive and restrictive. Supplemental ROEs set by the President, Secretary of Defense, or Combatant Commander are generally permissive in that they permit a specific tactic, weapon, or operation [31]. As a template for specific missions, Enclosure I of the standing rules details supplemental measures (and is primarily classified) and includes a list of weapons requiring approval by a Combatant Commander or higher [36].

All other supplemental ROEs generally seek to restrict action allowed under the SROEs or pre-existing supplemental ROEs [37]. For example, they may limit specific types of artillery, who may use certain weapons, or the targets that are acceptable to strike. However, supplemental ROEs only apply to mission accomplishment and do not restrict the use of force in self-defense. In 2010, when General Petraeus issued new ROEs for Afghanistan restricting

15 Under some circumstances, one or more of the following actions may demonstrate hostile intent: aiming or directing weapons; adopting an attack profile; closing within weapon release range; illuminating the commander's unit with radar or laser designators; passing targeting information; or laying or preparing to lay naval mines.

16 The formal definition of "passive defense" is "measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative" [33].

17 The formal definition of "active defense" is the "employment of limited offensive action and counterattacks to deny a contested area or position to the enemy" [34].

aerial bombardments and artillery strikes, he took care to remind commanders of their right to use force in self-defense [38].

In general, supplemental ROEs reflect policy judgments about how deployed forces should behave to best support national interests. Supplemental ROEs can be used elaborate on how the SROEs should be interpreted in situations likely to occur during a specific mission. For example, a given mission might call for deployed forces to interact with civilians. If such interactions are unfriendly (e.g. an encounter with an unarmed mob), the risk of escalating a conflict may be high, and so a supplemental ROE might direct that the unit should withdraw or use smoke to camouflage itself, but should not use its weapons to fire on the mob.

Because they are mission-specific, supplemental ROEs are an important focus of mission planning, which is a process that involves specific objectives, lists of targets to be attacked to support those objectives, and various courses of action and options for attacking each target. Pros and cons of attacking each target with each option are analyzed and commanders make decisions about which option is better under any given set of circumstances, or whether none are acceptable (at which point his or her staff must develop another option for consideration). Offensive cyber options have, in principle, the same status as offensive options in the physical domains such as land and air – the pros and cons of each option factor into the commander's decision.

Mission planning results in an operation plan, defined by DOD as "a complete and detailed joint plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment data" [39]. Mission planning may also take place long in advance of actual military action – in fact, it usually does. However, the mere fact that a mission has been planned in advance (and that possible options and courses of action have been identified) does not automatically mean that commanders have the authority to execute that mission.

Instead, commanders can take action only when they receive an explicit order from higher authority to do so. Such an order is called an execute order (or EXORD), which the DOD defines as "an order issued by the Chairman of the Joint Chiefs of Staff, at the direction of the Secretary of Defense, to implement a decision by the President to initiate military operations" [40].

As an example, consider a situation in which potentially hostile forces from Country X face U.S military forces on land. One important scenario of interest to the USA is how it would respond to a surprise large-scale attack by Country X across the zone separating the two forces. An effective US response would entail a great deal of preplanning – the plan for the response is designated in a formal operational plan, most likely containing supplemental ROEs. Execution of the actions contemplated in the plan would require an explicit order from the President or Secretary of Defense, and such an order would be transmitted as an EXORD. Nevertheless, under the SROEs, the commander of these forces may act in self-defense to a hostile act from Country X without additional authorization – and if that hostile act is large rather than small, the US response may well be large as well if that is needed to neutralize the immediate threat. But the commander would not be authorized to act on his own authority, that is, without an EXORD or other authority, to go beyond the needs of immediate self-defense and capture the capital of Country X. Of course, this hypothetical situation would become even more complex with the inclusion of allied and coalition partners.

Thus, it is important not to conflate the existence of operation plans with SROEs. Nevertheless, an execute order remains valid until either the mission is accomplished or the operation explicitly terminated [41], and under some circumstances, an execute order is for all practical purposes a "standing" order that grants authorities to act in certain ways in accordance with a given operation plan. Furthermore, because an operation plan describes actions that to be taken prior to actual conflict, the issuance of an execute order does not mean that actual conflict is about to break out.

Standing rules for the use of force

SRUF are similar to the SROEs in that they provide a general set of rules governing US military action. The primary differences lie in their intent and geographic applicability.

Unlike the SROE, which are essentially permissive in nature, SRUFs are inherently restrictive. Unless specific weapons and tactics are explicitly approved under the SRUF, they cannot be used without the authorization of the Secretary of Defense [42].

The SROEs apply to actions taken outside US territory, as well as to air and maritime homeland defense missions [31]. SRUFs govern military functions inside US territory. They include Defense Support to Civilian Agencies (DSCA), land homeland defense missions, and law enforcement/security measures at DOD installations. However, the SRUFs do not apply to the National Guard when it is operating in a state rather than federal status. The National Guard primarily acts as a "federally-recognized state government entity" and is generally called to service in support of state civil authorities [43]. Thus, each state has its own set of rules that guide the National Guard based on the laws of that state.[18]

DSCA offers one example of SRUFs application. In that mission, conventional forces from the Navy, Air Force, and Army were assigned to support civilian authorities with search and rescue, aid delivery, and peace-keeping.[19] SRUFs have not received much attention over the years because situations where DOD support to civil authorities infrequently involve the use of force.

Acknowledgements

C. Robert "Bob" Kehler retired from the United States Air Force in December 2013. Prior to his retirement, General Kehler was the Commander of United States Strategic Command. Herbert Lin is Senior Research Scholar for Cyber Policy and Security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University. Michael Sulmeyer is Director of the Cyber Security Project, Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University. All views expressed in this publication are only those of the authors.

C. Robert "Bob" Kehler thanks Theodore Richard for reviewing an early draft of this paper. Herbert Lin thanks Taylor Grossman for critical assistance. Michael Sulmeyer thanks Peter Pascucci for reviewing an early draft of this paper and Olivia Zetter for excellent research assistance.

This work was supported by the Cyber Policy Program of Stanford University's Center for International Security and Cooperation and the Hoover Institution.

References

1. Amos J, Petraeus D, Nagl J *et al*. Police in counterinsurgency. In: *The U.S. Army/Marine Corps Counterinsurgency Field Manual*, 1st edn. Chicago: University of Chicago Press, 2007, 233.

18 There is no standard term used by states for rules of force. Some refer to them as rules for the use of force (RUF), as used here; however, others use rules of engagement (ROE), and rules of interaction (ROI) [43].

19 See [44] and [45] for press accounts. See also [46].

2. Department of Defense. Terms and definitions: rules of engagement. In: *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, 2010–2016, 207. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (21 January 2017, date last accessed).
3. Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 2016.
4. II-Strategic Context. *Department of Defense Cyber Strategy*, Department of Defense, 2015, 11. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (21 January 2017, date last accessed).
5. Bellovin S, Landau S, Lin H. Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *J Cybersecurity* 2017;**3**.
6. Chapter 5, Appendix A, Standing Rules of Engagement. In: *Operational Law Handbook*, The International and Operational Law Department of the Judge Advocate General's Legal Center and School, 2015, 91 [A-2]. http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf (21 January 2017, date last accessed).
7. Enclosure L. *Standing Rules for the Use of Force for US Forces CJCSI 3121.01B*, Department of Defense Joint Chiefs of Staff, 2005. https://navytribe.files.wordpress.com/2015/11/cjcsi-3121-01b-enclosure-l.pdf (21 January 2017, date last accessed).
8. Chapter 5, Self AA. defense. In: *Operational Law Handbook*, The International and Operational Law Department of the Judge Advocate General's Legal Center and School, 2015, 91 [A-2]. http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf (21 January 2017, date last accessed).
9. National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Owens, W, Dam, K, Lin, H, (eds). Washington, D.C.: National Academies Press, 2009. http://www.nap.edu/catalog/12651.html (21 January 2017, date last accessed).
10. Air Force Material Command, Department of the Air Force. 70 – Cyber Control System. *FedBizOpps* (20 December 2007). https://www.fbo.gov/index?s=opportunity&mode=form&id=e80b7d909c5fa5107528a05bdf51d1bd&tab=core&_cview=1 (21 January 2017, date last accessed).
11. Transitional Cyber C2 Construct. In: *Operations Order 11-002, Operation Gladiator Shield*, United States Cyber Command, 2011, 44. http://nsarchive.gwu.edu/dc.html?doc=2692120-Document-12 (21 January 2017, date last accessed).
12. III-Strategic Goals. In: *Department of Defense Cyber Strategy*, Department of Defense, 2015, 14. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (21 January 2017, date last accessed).
13. Libicki M. *Crisis and Escalation in Cyberspace*. Santa Monica, CA: RAND Corporation, 2012.
14. 1.11.5.1 Responding to an Imminent Threat of an Attack. In: *Department of Defense Law of War Manual*, Department of Defense, Office of General Counsel, 2016, 46–47. http://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf (21 January 2017, date last accessed).
15. DeWeese G. Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence. In: *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, Estonia, 2015, 81–92. NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia. https://ccdcoe.org/cycon/2015/proceedings/06_deweese.pdf (21 January 2017, date last accessed).
16. Tibori Szabó K. Introduction. In: *Anticipatory Action in Self-Defence: Essence and Limits under International Law*. New York: Springer, 2011, 6–8.
17. Ducheine P, Gill T. Anticipatory self-defense in the cyber context. *Int L Stud* 2013; **89**:452.
18. Ducheine P, Gill T. Anticipatory self-defense in the cyber context. *Int L Stud* 2013; **89**:438–71.
19. 2.4.2 Examples Where Proportionality is Reflected in Law of War Rules. In: *Department of Defense Law of War Manual*, Department of Defense, Office of General Counsel, 2016, 61–62. http://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf (21 January 2017, date last accessed).
20. I-Introduction. *Department of Defense Cyber Strategy*, Department of Defense, 2015, 5. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (21 January 2017, date last accessed).
21. Secretary of Defense Ash Carter, Chairman of the Joint Chiefs of Staff General Joseph F. Dunford. Department of Defense Press Briefing by Secretary Carter and Gen. Dunford in the Pentagon Briefing Room. 29 February 2016. http://www.defense.gov/News/Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the (21 January 2017, date last accessed).
22. III-Strategic Goals and IV-Implementation Objectives. *Department of Defense Cyber Strategy*, Department of Defense, 2015, 14 and 24–26 (last accessed 21 January 2017). http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (21 January 2017, date last accessed).
23. Center for Army Lessons Learned. *Escalation of Force Handbook*. Fort Leavenworth, KS: United States Army Combined Arms Center, 2007.
24. Bronk C, Tikk-Ringas E. The cyber attack on Saudi Aramco. *Survival* 2013; **55**:85.
25. Meserve J. Staged cyber attack reveals vulnerability in power grid. *CNN*, 26 September 2007. http://www.cnn.com/2007/US/09/26/power.at.risk/index.html?iref=topnews#cnnSTCVideo (21 January 2017, date last accessed).
26. National Research Council. *Toward a Safer and More Secure Cyberspace*, Goodman, S and Lin, H (eds). Washington DC: National Academies Press, 2007.
27. International and Operational Law Department. The Judge Advocate General's Legal Center & School. *Operational Law Handbook*. Charlottesville, VA: The Judge Advocate General's Legal Center & School, U.S. Army, 2015. http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf (21 January 2017, date last accessed).
28. Deployable Training Division of the Joint Staff J7. Authority to Use Force. In: *Insights and Best Practices Focus Paper – Authorities*, Joint Staff J7, 2016, 9. http://www.dtic.mil/doctrine/fp/fp_authorities2016.pdf (21 January 2017, date last accessed).
29. Chapter 5, Rules of Engagement. In: *Operational Law Handbook*. The International and Operational Law Department of the Judge Advocate General's Legal Center and School, 2015, 82. http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf (21 January 2017, date last accessed).
30. Chapter 5, Rules of Engagement. In: *Operational Law Handbook*, The International and Operational Law Department of the Judge Advocate General's Legal Center and School, 2015, 81–83. http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf (21 January 2017, date last accessed).
31. Chapter 5, Rules of Engagement. In: *Operational Law Handbook*, The International and Operational Law Department of the Judge Advocate General's Legal Center and School, 2015, 84. http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf (21 January 2017, date last accessed).
32. Chapter 5, Appendix A, Self Defense. In: *Operational Law Handbook*, The International and Operational Law Department of the Judge Advocate General's Legal Center and School, 2015, 91 [A-2]. http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf (21 January 2017, date last accessed).
33. Department of Defense. Terms and Definitions: Passive Defense. In: *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, 2010–2016, 181. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (21 January 2017, date last accessed).
34. Department of Defense. Terms and Definitions: Active Defense. In: *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, 2010–2016, 1. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (21 January 2017, date last accessed).
35. Amos J, Petraeus D, Nagl J, *et al*. Appendix D-Legal Considerations. In: *The U.S. Army/Marine Corps Counterinsurgency Field Manual*, 1st edn. Chicago: University of Chicago Press, 2007, D-8.
36. Solis G. Rules of Engagement-Formulating Mission-Specific ROE. In: *The Law of Armed Conflict-International Humanitarian Law in War*. New York: Cambridge University Press, 2010, 500.

37. Chapter 5, Rules of Engagement. In: *Operational Law Handbook*, The International and Operational Law Department of the Judge Advocate General's Legal Center and School, 2015, 81 and 84. http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf (21 January 2017, date last accessed).
38. Michaels J. Petraeus reloads rules of engagement. *USA Today*. 5 August 2010. http://usatoday30.usatoday.com/news/world/afghanistan/2010-08-05-airstrikes05_ST_N.htm (21 January 2017, date last accessed).
39. Department of Defense. Terms and Definitions: Operation Plan. In: *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, 2010–2016, 177. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (21 January 2017, date last accessed).
40. Department of Defense. Terms and Definitions: Executive Order. In: *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, 2010–2016, 83. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (21 January 2017, date last accessed).
41. Joint Operation Planning, Joint Publication *5-0*, Department of Defense, 2011. http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf (21 January 2017, date last accessed).
42. Chapter 5, Rules of Engagement. In: *Operational Law Handbook*, The International and Operational Law Department of the Judge Advocate General's Legal Center and School, 2015, 86. http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf (21 January 2017, date last accessed).
43. II-Rules for the Use of Force for the National Guard. In: *Domestic Operational Law Handbook for Judge Advocates*, Center for Law and Military Operations of the Judge Advocate General's Legal Center and School, 2013, 191. http://www.loc.gov/rr/frd/Military_Law/pdf/domestic-law-handbook-2013.pdf (21 January 2017, date last accessed).
44. Arana-Barradas L. Air Force rescues top 4,000 mark. *U.S. Air Force*. 8 September 2005. http://www.af.mil/News/ArticleDisplay/tabid/223/Article/133434/air-force-rescues-top-4000-mark.aspx (21 January 2017, date last accessed).
45. Commander, U.S. 2nd Fleet Public Affairs. Norfolk Ships Deploy to Support Hurricane Katrina Relief Efforts. *U.S. Navy*. 31 August 2005. http://www.navy.mil/submit/display.asp?story_id=19826 (21 January 2017, date last accessed).
46. Solis G. Rules of engagement-standings rules of force. In: *The Law of Armed Conflict-International Humanitarian Law in War*. New York: Cambridge University Press, 2010, 494.