JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 3(1), 2017, 19–28
doi: 10.1093/cybsec/tyw016
Advance Access Publication Date: 18 February 2017
Research paper

Research paper

A cyber SIOP? Operational considerations for strategic offensive cyber planning

Austin Long*

Columbia University

*Corresponding author: E-mail: al2866@columbia.edu

Received 20 December 2016; accepted 20 December 2016

Abstract

Most discussion to date about offensive cyber operations has focused on the theoretical and strategic rather than operational level of analysis. This mirrors the nuclear age, where critical operational questions were neglected in public discussion until very late in the Cold War. Yet these questions are critical for both nuclear and cyber operations, so analysis that neglects them has little bearing on policy questions. An examination of the planning, targeting, and command and control aspects of offensive cyber operations in the US context provides a starting for a more fruitful assessment of offensive cyber.

Key words: cyber planning; strategy; SIOP

For the first three decades of the nuclear age, discussion of nuclear strategy (particularly academic discussion) overwhelmingly focused on theoretical aspects of deterrence and certain stylized properties of weapons (yield, accuracy, etc.). Critical issues of command, control, communications, and intelligence (C3I) as well as targeting and planning operations were frequently ignored or elided. This was in part due to dearth of information available about these topics, sometime even for those with security clearances (on the limitations even analysts with security clearances faced, see [1–3]). Yet it also reflected a general view that nuclear weapons were radically different than conventional weapons [4].

Beginning in the 1970s scholars began to appreciate the importance of C3I, targeting, and operational issues for nuclear war [5, 6]. This appreciation greatly improved the discourse on nuclear strategy as discussion became less ethereal even at the unclassified level. By the end of the Cold War, scholars were able to attempt unclassified models of the Single Integrated Operational Plan (SIOP), the US nuclear war plan [7].

Discussion about cyberwar and offensive cyber operations (OCO) have thus far mirrored the early nuclear age, often neglecting C3I and operational issues in favor of more theoretical debates [8–10]. This essay is an effort to move discussion of strategic cyber warfare toward operational and tactical considerations. It takes the lexicon of nuclear operations as its starting point, while acknowledging the differences between nuclear and cyber operations. It does so from a US perspective, as the author's experience is with the US military and intelligence communities. Those communities are also not incidentally the world's most capable cyber actors [11] (many observers have concluded the Equation Group is affiliated with, if not a component of, the US National Security Agency). However, much of the logic should apply to all forms of strategic OCO.

The article proceeds in six parts. First, it describes the main categories of targets for OCO, and the nature of effects cyber operations could generate on those targets. Second, it discusses the intelligence requirements for OCO. Third, it argues that the relative ease of offense versus defense (the offense–defense balance) for OCO, an important component of strategic planning, varies depending on the target. Fourth, it describes the C3I requirements for OCO in the context of strategic warfare. Fifth, it discusses the distinction between theater and strategic cyber operations, which has C3I implications. It concludes with thoughts on the future of strategic OCO.

The focus of this article is particularly on strategic OCO for military purposes. This distinguishes it from OCO for covert action or pure intelligence collection purposes. However, given the paucity of strategic OCO to date, some of the illustrative examples draw on historical cases of OCO for covert action (e.g. Stuxnet).

Targeting OCO: strategic guidance for planning

Borrowing from the nuclear lexicon, there are two broad categories of targets for OCO: countervalue and counterforce. Countervalue targets are those without significant military utility but are of significant other value to the targeted state. Examples include general industrial targets, financial systems, etc. Countervalue targeting is typically considered to be consonant with a strategy focusing on

deterrence (or possibly compellence) by punishment – that is, making the cost of taking (or not taking) an action higher than the expected value of the alternative course of action [12] (for a short primer on deterrence theory, generally see [1]).

Counterforce targets are those with significant military utility. This covers a wide array of targets, from C3I systems to nuclear and conventional forces to some war-supporting industries (e.g. a munitions plant). Counterforce targeting has potential utility for not only deterrence by punishment but also deterrence by denial. Deterrence by denial seeks to deter a potential adversary from taking action by increasing the risk that action will simply fail to achieve an objective. Many states place some value on their military capabilities, so holding them at risk can impose costs while at the same time increasing the risk the state will not achieve military objectives [12,13].

There are a variety of targets that straddle the divide between the two categories, at least in some contexts. For example, commercial electrical power production facilities and civilian communications infrastructure may have significant nonmilitary utility but also military utility in some contexts. Some states may rely heavily on both to support integrated air defense operations, for example. Conversely, targeting enemy leadership and internal security services may have military utility but potentially even greater nonmilitary value in terms of regime survival.

Strategic OCO planners will require guidance from the National Command Authority (NCA) on the objectives and priorities of targeting. In the nuclear realm this is provided in a series of documents, beginning with the President's guidance through the National Security Council, which is then elaborated by the Secretary of Defense's Nuclear Weapons Employment Policy (NUWEP). These documents are then used by the Chairman of the Joint Chiefs of Staff to develop the Nuclear Supplement to the Joint Strategic Capabilities Plan (JSCP-N), which gives detailed instruction to Strategic Command (STRATCOM) on targeting and planning requirements [14].

It is unclear at the unclassified level if a similar set of guidance documents exists to guide strategic OCO. News reports indicate that some Presidential guidance on developing a target list for OCO was provided in 2012 by Presidential Decision Directive (PDD) 20 [15]. However, it is not apparent whether a cyber-equivalent of the NUWEP and JSCP-N exist. Whether they do or not at present, it is worth considering what guidance such documents must provide to strategic OCO planners.

First, guidance documents should provide the objectives to be achieved through strategic targeting of OCO. In the nuclear case those objectives, in available declassified versions, have been 3-fold. First, to deter attack or coercion based on the threat of attack on the USA and its allies. Second, to control escalation if deterrence fails. Escalation control is to be achieved through limiting the scope of response and selecting targets that leave some adversary targets hostage to the threat of future attack. Third, if escalation control fails, to conduct general war to achieve maximum US power relative to the adversary. This is to be achieved by destroying targets critical to the adversary's postwar status while limiting damage to the USA and its allies through counterforce operations and retaining a reserve force for use after the conclusion of hostilities [16].

For a cyber-equivalent to the SIOP (i.e. a plan for strategic OCO), planners need similar objectives. Deterrence is an obvious parallel objective between nuclear and cyber but deterrence of what? During the Cold War strategic nuclear forces were intended to deter both nuclear and conventional attacks, while more recently unclassified guidance "directs DOD to strengthen non-nuclear capabilities and reduce the role of nuclear weapons in deterring non-nuclear attacks" [17]. Are strategic OCO intended primarily to deter adversary OCO or are such operations part of a broader set of deterrent capabilities, including nuclear forces? The latter seems more likely but this is a policy choice different administrations may answer differently.

If deterrence fails, OCO planners need subsequent objectives. Here the parallel with nuclear operations, at least those from the Cold War context, may be less obvious. Is the next objective for strategic OCO the control of escalation? It could be but this might vary by adversary and scenario. Failure of deterrence regarding a great power like Russia or China might lead to a subsequent objective of escalation control but North Korea or Iran might be different, with the objective being the prompt neutralization of adversary strategic capabilities in order to limit (or eliminate) damage from enemy attack.

OCO could be a component of either objective, but would be planned very differently. For escalation control, planners would need to define targets that punish the adversary and/or deny objectives in order to demonstrate US resolve. Yet the targets would have to be of a nature unlikely to lead to further escalation by the adversary. The need to strike this balance – producing effects sufficient to show resolve without risking escalation – will be challenging to policymakers and planners alike. Inadvertent escalation was a major worry in the late Cold War with conventional and nuclear forces – a concern that is now returning in East Asia and potentially the eastern and southern flank of the North Atlantic Treaty Organization (NATO) [18–21]. The addition of OCO further compounds this problem by creating new pathways to inadvertent escalation.

A historical parallel to OCO and inadvertent escalation was the concern about the impact of electronic warfare (EW) in a conventional battle in Europe on Soviet early warning of a US strategic nuclear attack, particularly one directed at the Soviet strategic nuclear arsenal [18]. EW in this context was not intended to threaten Soviet strategic forces, but could nonetheless generate pressure for Soviet nuclear use as they became fearful their forces were vulnerable.

Soviet exercises reflected this fear. In a 1984 Soviet strategic exercise, US bombers exploited damage to Soviet air defense as well as the massive volume of electronic warfare to strike key Soviet command centers. This initial attack was promptly followed by a devastating attack on Soviet strategic nuclear forces [22]. Thus conventional air operations, including electronic warfare, in an actual war may have made the Soviets extremely concerned about the survival of their nuclear forces and thus potentially pressured them to use nuclear weapons first.

Strategic OCO could create similar fears, as attacks on even nonmilitarily critical systems (e.g. power supplies) could impact military capabilities or stoke fears that military networks had likewise been compromised. Indeed, OCO effects could be more escalatory than traditional electronic warfare, which even if it compromises air defense is nonetheless generally observable – radar operators will often know they are being jammed even if they can do nothing about it. OCO, if done well, could compromise systems without the target knowing. An adversary thus might not be able to distinguish between a system failure due to OCO and a natural system failure. In a crisis or conventional war, if some component of an adversary's command and control failed it could easily be misinterpreted as successful OCO, creating escalatory pressures. Targeting strategic OCO for escalation control without risking inadvertent escalation may thus be a major planning challenge.

In contrast, strategic OCO may be very useful for achieving damage limitation objectives, particularly against regional powers like North Korea. Indeed former Deputy Secretary of Defense John

Harvey has called for a comprehensive effort to negate North Korea's nuclear arsenal, including:

> Cyber capabilities to disrupt warhead arming and firing systems, or cause flaws to be introduced into warhead designs, so that any arriving warheads are duds. On this last point, foreign "assistance" to North Korea's nuclear program is a problem, but it is also an opportunity. Under such conditions, North Korea's leaders would no longer "own" their nuclear weapons — in a sense, we would. A bit fanciful? Not necessarily. The technologies, subsystems and capabilities exist today to address each one of these goals notwithstanding the need for a bit of luck here and there. It is well within the realm of technical possibility [23].

Thus, the target choice would be less restricted in planning for damage limitation than in escalation control – essentially everything would be fair game. Yet this has escalation risks unique to OCO – establishing the accesses needed for OCO could be escalatory, as discussed in the next section.

A final objective might be the maintenance of a cyber "reserve" force. This may or may not be important to policymakers and planners, as the need to maintain a reserve would depend substantially on the uniqueness of accesses and exploits as well as the importance of the conflict. If the exploits and accesses are unique or mostly unique to the target – e.g. an indigenous Iranian air defense server system – then there may be little technical reason to reserve an attack capability for future conflict. On the other hand, a more widely applicable OCO capability in terms of exploits and accesses – e.g. a widely used supervisory control and data acquisition (SCADA) system – might be best kept in reserve. Much would depend on the context of use, and hence planners would need to think through options as related to both overall objectives and specific option planning discussed below.

In addition to overall objectives, guidance to strategic OCO planners should include direction on desired attack structure and related operational priorities. In the nuclear context, attack structure in available declassified records had four elements: Limited Nuclear Options (LNOs), Selected Attack Options (SAOs), Major Attack Options (MAOs), and Regional Nuclear Options (RNOs) [16]. This structure provides a useful starting point for thinking about the structure of strategic OCO.

LNOs were intended as the initial mechanism for nuclear response while controlling escalation. While details of the nature of any preplanned LNOs are not available at the unclassified level, the guidance indicated they should signal US commitment to a conflict and should focus on improving the military balance in a local conflict. A cyber-equivalent, perhaps a Limited Cyber Option (LCO), would target adversary systems of local military utility while attempting to limit the risk of escalation. The latter objective would require both a quantitative limit on the size of the attack and a qualitative limit on the military value of the target.

An example target for an LCO might be a system that contributes to adversary offensive targeting capability. This could be an adversary over the horizon targeting system, such a satellite constellation or over the horizon radar. Such systems are a vital part of an adversary's ability to track and target US forces at long range, but could potentially be discretely targeted in a way unlikely to impair adversary strategic early warning or attack assessment.

In terms of scale, the Stuxnet attack on Iranian centrifuges would be an exemplary LCO. It was confined to specific industrial control systems used by Iranian centrifuges in a limited number of facilities. Even then the malware spread beyond the targeted facilities but did not cause widespread collateral effects [24]. To be clear Stuxnet was not an LCO, having been intended to achieve its limited aims in a covert manner, while an LCO could be much more overt. However, Stuxnet demonstrates the ability to conduct OCO in a very discrete and discriminate fashion.

In contrast to an LNO a nuclear SAO would be a significantly larger target set, such as an adversaries long-range strike aircraft. This would require comprehensive targeting of all airbases, including dispersal bases. A cyber SAO intended to achieve the same effect would target both airbase air traffic control and logistic systems as well as the avionics of adversary strike aircraft (all to the extent possible). The risk of escalation from SAOs is higher than that associated with LNOs (indeed an SAO could be thought of as an aggregation of LNOs). Yet the military impact would be substantially higher, providing policymakers with stronger options.

Cyber SAOs also potentially provide unique opportunities for escalation that would be more difficult or even impossible for conventional or nuclear forces. One might be an SAO targeting adversary capabilities for information and population control, such a regime controlled media outlets, internal security databases, and censorship/surveillance capabilities. A cyber SAO against this target set offers the ability to create effects without civilian loss of life and potentially the ability to introduce new information into the adversary state. This could be either false information (e.g. corrupting internal security databases by adding fictitious information) or true information (e.g. a more accurate representation of events in regime media).

A possible similar cyber SAO would target adversary OCO capabilities. This would include C3I for OCO along with specific facilities known to generate OCO exploits or tools. While OCO can be conducted in a distributed fashion, there are nonetheless likely to be a variety of critical nodes in C3I. For example, as of 2013, a large number of Chinese cyber operations originated from a single building [25].

Cyber SAOs also present the potential opportunity for countervalue attacks with very limited civilian collateral damage (in terms of civilian deaths). An example could be an SAO on an adversary financial system – banks, capital markets, etc. Another could be electrical power production, though this would likely cause indirect civilian deaths from the loss of power to critical systems with limited back up (traffic control, for example).

MAOs represent the ultimate escalatory options for policymakers. If SAOs are analogous to aggregated limited options, then MAOs are aggregations of SAOs. An example would be a comprehensive attack on all adversary military systems, including nuclear, conventional, space, and cyber. Additionally, MAOs in the nuclear context can include attacks on countervalue targets, so presumably any countervalue cyber SAOs could be combined into an MAO.

Finally, RNOs are intended to respond to theater contingencies with theater forces. As discussed below, theater cyber forces are growing so the possibility of Regional Cyber Options (RCOs) could be growing as well. Yet part of the desire for RNOs was the belief, correct or not, that responses from theater forces would be seen as less escalatory than responses with strategic forces. It is not clear adversaries will even be able to distinguish OCO conducted by "theater" forces from those conducted by "strategic" forces, particularly given that cyber force assigned to a regional combatant commander may not be collocated with that commander.

Yet RCOs may be distinguishable by limiting geographic scope and effect rather than by geographic origin. It may therefore fill a gap between LCOs and cyber SAOs. For example, an RCO might be created as part of a regional combatant commander's war plan that attacks a broad target set, such as air defense systems, in a limited geographic area (such as the most likely point for conventional conflict with an adversary). While not as distinct from strategic OCO as

its nuclear equivalent, RCOs of this type would thus allow a commander to present the NCA with an option combining military utility with somewhat limited escalatory risk.

In addition to providing guidance on types of cyber options, policymakers must provide guidance on damage expectancy for cyber options. Is the goal of a given option to produce relatively transient and/or reversible effects? If so, within what parameters (e.g. disrupt the functioning of a system for hours, days, weeks, etc.)? If not, how much effort should OCO planners put into ensuring effects are difficult to reverse, with the high end for such expectancy being physical destruction of critical system components?

This guidance will likely be affected by how policymakers envision cyber options interacting with other military options. One example would be options targeting adversary nuclear forces. It is unlikely, though not impossible, policymakers would be willing to target adversary nuclear forces with cyber options alone. Cyber options targeting adversary nuclear forces (and attendant C3I) would therefore only be expected to achieve transient effects and, ideally, improve the ability of conventional or nuclear strikes to destroy those nuclear forces (e.g. by revealing the location of mobile nuclear forces while disrupting their ability to move and launch). Even a transient effect of a few hours in this instance could vastly improve the efficacy of other military options. Such counter-C3I options against Soviet strategic targets using electronic warfare were apparently developed during the late Cold War [26,27].

The countervalue equivalent of this damage expectancy is a denial of service type effect. Here the target system held at risk would be unavailable for some period of time but would eventually return to full operational status. The 2007 wave of distributed denial of service (DDoS) attacks on Estonian government and commercial websites is an example of this level of damage expectancy [28,29].

At the other end of the spectrum, a cyber SAO targeting regime information and population control mechanisms might ideally produce permanent effects, at least for some systems. Permanent loss of servers used to maintain censorship/surveillance programs would impose very significant costs on any adversary that values such programs. The same would be true of servers associated with adversary OCO.

The countervalue equivalent of this damage expectancy is the physical destruction or permanent disabling of the target system. One reported example is the targeting of a German integrated steel mill reported in 2014. An operation targeting the mill's industrial control systems led to an inability to safely shut the mill down and "... massive damage to the whole system" [30]. Server and computer damage accompanying the North Korean OCO against Sony is also at this end of the damage expectancy spectrum [31].

Along with the spectrum of effects ranging from disruption/denial of service to physical destruction, OCO also presents an additional category of potential "damage" expectancy distinct from any offered by nuclear or conventional weapons. This is the opportunity for deception by introducing false information into adversary networks [32]. Successful deception could be more militarily useful for some targets than disruption or destruction. For example, adversary systems that provide position, navigation, and timing (PNT) information will likely enable precision strike capabilities. The premier examples are satellite-based PNT systems like the US Global Positioning System (GPS) and similar Russian GLONASS and Chinese Beidu systems (see overview of GPS control in [33]). Such systems rely on ground control stations to precisely monitor and control satellites, which in turn transmit signals to users.

Simply disrupting or destroying PNT systems would force adversaries to use alternative methods, such as shifting to nonprecision munitions, which would degrade performance. But subtly altering data in the monitoring and control system might degrade performance more as the adversary would be unaware of the problems in the PNT system and therefore continue to rely on it even as it provided inaccurate data. Thus rather than moving from accurate to less accurate weapons (if PNT were disrupted or destroyed), the adversary would have accurate weapons that consistently missed their aim point by small but militarily important distances (a dozen meters perhaps) without initially understanding why such weapons were not destroying their targets.

Before proceeding it is worth noting one of the difficulties of developing cyber options for deterrence is the limitation on credibly communicating those options to adversaries. For example, imagine the USA had a very credible cyber option to permanently disable most or all of the servers supporting the so-called "Great Firewall" of China [34]. This option might have significant deterrent value if communicated but as noted in the next section, developing such an option would entail very detailed intelligence development of the targeted servers and exploiting vulnerabilities in the server system to obtain access. Credibly communicating the ability to attack this system would, in addition to potentially provoking China, likely reveal aspects of the access method. At a minimum it would increase Chinese vigilance in looking for vulnerabilities in the system. In other words, revealing the deterrent threat might fully or partially vitiate its efficacy– in contrast to most nuclear or even conventional deterrent threats.

Targeting OCO: intelligence requirements

While the intelligence requirement for nuclear options is not trivial, it is relatively straightforward. The central requirement for nuclear targets is a list of targets meeting the criteria required in the guidance noted above. This has been known as the National Strategic Targets List, a database of thousands of relevant target [35].

Each target on the list then has specific intelligence requirements. These include the nature of the target, the precise location of the target (for fixed targets anyway), the vulnerability of the target to nuclear effects, and depending on the target, the extent of active defenses that must be suppressed to reliably attack the target. During the Cold War among the most difficult fixed targets were underground hardened command and control sites around Moscow, a city protected by extensive active defenses [36]. Yet the intelligence requirements once the sites were located were relatively modest.

In contrast, the intelligence requirements for cyber options are immense, as the delivery mechanism is entirely dependent on intelligence collection. First, the target and its vulnerabilities must be identified, then a malware payload exploiting those vulnerabilities developed and access routes into the target established (for an overview of vulnerability, payload, and access requirements see [37]). This can be extraordinarily difficult, even for advanced cyber actors, depending on the characteristics of the target [38]. Many targets may not be connected to any external networks or may function on dedicated land networks, which does not present an insurmountable barrier but does require very extensive intelligence development to cross [39]. Other targets may only be accessible through radio frequency operations. The US Air Force has publicly acknowledged using its Compass Call jamming aircraft to target a variety of networks for exploitation [40].

For example, cyber options targeting missile systems (e.g. surface to air missiles or ballistic missiles) would require an understanding of both the C3I network supporting missile operations and ideally

the missile system itself. The latter would require foreign military exploitation – the acquisition and experimentation with examples of the system itself. This is a capability the USA is investing heavily in, but does require examples of the foreign technology (or intelligence access to detailed technical specifications) [41].

For some systems this may be relatively easy for the USA. As an example, Greece, a NATO ally, has acquired the Russian S-300 surface to air missile (NATO designation SA-10 Grumble). Exploitation of the export variant of S-300 would be trivially easy. During the Cold War the USA also benefited from exploitation of aircraft from defectors, such as the 1976 defection of Viktor Belenko in an advanced MiG-25 Foxbat interceptor [42]. In other cases intelligence from other sources provided similar insight, such as Adolf Tolkachev's detailed technical information on Soviet airborne radars [43] (for a contrary argument on the importance of Tolkachev, see [44]).

For many systems of interest exploitation of a full system will be impossible. For example, no samples of adversary intercontinental ballistic missiles (ICBMs) are likely to be available to exploitation. Yet subsystems or analogous systems could be available. For example, the Soviet/Russian Topol and Topol-M (NATO designation SS-25 Sickle/SS-27 Sickle-B) mobile ICBMs use a transporter erector launcher (TEL) based on more widely distributed designs that originated from a firm based in what is now Belarus [45]. This could potentially permit development of accesses and exploits of these systems.

The challenge of targeting intelligence and access development for some targets helps clarify one of the persistent questions about OCO – is cyber an offense- or defense-dominant operating environment? (an overview and critique of the offense–defense literature in political science can be found in [46] and [47]). Many authors argue the cyber environment is offense dominant and therefore fraught with risks of escalation and security dilemmas. In this environment to improve one's own security through cyber capabilities imperil others, leading to arms races and instability [10].

Yet others have observed that the conduct of OCO is often enormously challenging. Erik Gartzke and Jon Lindsay highlight the fact that deception, noted above as an effect of OCO, can be used by a clever defender to cripple offensive activity [32]. Some have also noted the enormous effort needed to establish the accesses and exploits required for OCO against hard targets such as the SCADA systems in Iran's Natanz uranium enrichment plant [48]. Even the use of airborne platforms like Compass Call to establish access creates a high barrier to entry for OCO – only a handful of nation-states operate such sophisticated electronic warfare assets [49]. For these observers, the cyber environment could very well be defense dominant, with only very well-resourced actors capable of any but the most rudimentary OCO.

How to reconcile these divergent perspectives? First, one of the issues on assessing the offense–defense balance in the cyber-operating environment is different terminology between technologists and hackers on one side and political scientists and defense analysts on the other (thanks to Herb Lin for helping me understand this key difference in terminology across communities). Technologists often refer to offense as dominant if, given sufficient resources and time, an attacker can penetrate a system. This seems to be the terminology used in a 2013 Defense Science Board Report that claimed "With present capabilities and technology it is not possible to defend with confidence against the most sophisticated cyber attacks" (p. 1) [50]. The report classifies such sophisticated attackers as those that "… can invest large amounts of money (billions) and time (years) to actually create vulnerabilities in systems, including systems that are otherwise strongly protected … today limited to just a few countries such as the United States, China, and Russia" (p. 2) [50].

Yet when political scientists refer to the offense as dominant, they mean the offense is, dollar for dollar, easier than defense (as Charles Glaser and Chaim Kaufmann characterize it, the offense–defense balance is "… the ratio of the cost of the forces that the attacker requires to take territory to the cost of the defender's forces" [51]). If an attack requires years of work and billions of dollars to overcome a defense hypothetically costing millions of dollars, political scientists would characterize the environment as highly defense dominant. Defense dominance does not therefore mean offense is impossible – it just means attackers will have to spend disproportionately relative to the defender to achieve success.

The Defense Science Board report notes a variety of defensive measures can, at manageable cost, thwart even "… actors who are organized, highly technical, proficient, well funded professionals working in teams to discover new vulnerabilities and develop exploits" (chapter 8; quotation on p. 22) [50]. Moreover, even for the most sophisticated attackers (which the report terms Tier V-VI) these defenses "… when properly deployed, they make an attacker's task of moving data throughout the systems, while remaining undetected, much more difficult. Our goal is to raise the costs for the Tier V-VI attackers to succeed, limiting the number of operations they can afford to attempt" (p. 64) [50]. This assessment seems to accord with a political scientist's definition of defense dominance. Thus the same report argues high confidence defense is impossible against sophisticated actors, but relatively inexpensive efforts can thwart most attackers and limit attack options even for the most sophisticated. Clarity of terminology therefore matters a great deal – for purposes of this discussion offense dominant means it is cheaper on the margin to attack than defend not just that an attacker with enough time and money will get through.

The offense–defense balance as it pertains to OCO should therefore not be taken as a given for the entire operating environment. Rather, borrowing from the work of Stephen Biddle, the offense–defense balance for OCO should be conceived at the "operational" rather than environmental level [47]. The offense–defense balance is likely to be highly dependent on the target and objectives of OCO.

For example, imagine an air defense system connected by a combination of dedicated fiber optic lines and encrypted microwave datalinks. OCO against such a system would be possible but just establishing access might require some combination of physical operations to insert corrupted hardware into the fiber system or the actual radar/missile systems, kinetic attack against fixed nodes, and advanced electronic attack against the datalinks (probably airborne). Developing the malware payload would likewise require obtaining some sample of the code used in the system.

This is no doubt possible. A news report on one such program, the US Air Force's Project Suter, describes "the magic":

> After pinpointing the target antennas, Suter then performs its real magic – beaming electronic pulses into the antennas that effectively corrupt, if not hijack, the processing systems that present the enemy operators with their physical picture of the battlefield. Unlike classic jamming or EMP Electromagnetic Pulse attacks, these data streams do not flood enemy electronics with excess "noise" or power, but instead insert customized [*sic*] signals, including specialized [*sic*] algorithms and malware, into the vulnerable processing nodes [52,53].

The introduction of malware from Suter sounds like OCO and according to news reports the use of OCO for air defense

suppression was considered in 2011 for both the raid into Pakistan that killed Osama bin Laden and the Libya air campaign. It is not clear if these options were Suter based or much more extensive. OCO options were apparently rejected for a variety of reasons, including the timeline to prepare options (a testimony to the need for extensive intelligence preparation) and the existence of other options for defense suppression [54,55].

Yet if Suter and similar programs require hundreds of millions if not billions of dollars of investment and lengthy preparation to work against even relatively unsophisticated air defenses like Libya and Pakistan one can hardly claim these OCOs are offense dominant. A similar argument can be made about the Stuxnet attack. Offense is possible against targets with limited or no connectivity to the outside world but the defense will be dominant. Even modest efforts at defense make OCO against these targets impossible for all but the most capable (and patient) cyber attackers.

In contrast, commercially available systems with frequent or continuous connection to commercial communications (e.g. phone, fiber, or Bluetooth connections) are likely to be relatively easy targets for OCO. Here the offense may be dominant, particularly for reasonably sophisticated attackers capable of doing even modest reconnaissance (on social media, for example). This includes a variety of important targets, including the SWIFT system of interbank transfers as demonstrated by the recent cyber heist from the central bank of Bangladesh [56].

There are several insights to the limits of OCO that can be derived from general understanding of intelligence requirements. First, the ability to develop new OCO options during a crisis in anything like real time – a process STRATCOM refers to as "adaptive planning" – will be circumscribed [57]. Accesses to systems will, in most if not all instances, require pre-crisis exploitation. If this exploitation has not taken place then OCO options will frequently just not be available.

However, this will likely vary by target. Targets where offense dominates – mostly countervalue targets like SWIFT – may be significantly easier for adaptive planning. Payloads focused on widely used commercial software could be stockpiled (and maintained as software is upgraded or patched) for use in adaptive planning. Access to systems frequently or continually connected to commercial communications could potentially be established relatively quickly (days rather than months), making adaptive planning of countervalue OCO options possible. Where defense dominates – mostly counterforce targets like air defense – adaptive planning may be an impossibility on anything like crisis or conflict timelines.

Second, given the requirements for access, the number of cyber options that can be developed will be limited relative to nuclear or conventional options. As noted, for any specific target of nuclear or conventional options, the intelligence requirements are limited, while attack systems are highly fungible – the same nuclear weapon can be used to attack a wide array of targets. In contrast, accesses and vectors for cyber OCO are not likely to be very fungible. An exploit attacking communications links for a surface to air missile system may provide little or no utility for attacking a ballistic missile (unless perhaps they use very similar transport systems).

The combined limits on adaptive planning and fungibility between accesses and exploits means policymakers must provide much more detailed guidance on priorities to OCO planners. Thus if policymakers want to be able to hold electrical power generation rather than banking at risk with OCO, this level of specificity must be provided in guidance to OCO planners. Planner can then prioritize target development for these systems over, for example, adversary information and population control. This will be less true for many countervalue targets but will certainly be the case with many counterforce targets.

In addition to guidance, OCO planners must be given authorities required to develop access and exploitation of desired targets. Attempting to establish access, if discovered, can potentially be provocative so policymakers must measure the utility of any given OCO option against the escalation risk not just of executing the option but simply developing accesses for it. For example, adversary reaction to detected effort to access national level C2, including nuclear C2, could be extremely provocative if discovered.

According to open source reports, the USA may have such an opportunity now. A Chinese defector may have provided the USA with extensive information on the security of Chinese leadership facilities and the Chinese nuclear C2 [58]. This could allow the USA to develop cyber options against such targets – yet the escalatory risk of doing so may be large given the possibility efforts to develop access and exploits could be discovered.

In contrast, many countervalue targets will likely be only modestly provocative, as penetrations are relatively common. Balancing the potential utility of OCO options against both the intelligence investment required to develop access and the risk of attempting to develop access presents a major challenge, particularly relative to development of nuclear and conventional options. This balancing merits a major interagency review, akin to similar efforts in the nuclear realm during the 1970s or more recent efforts conducted as part of Nuclear Posture Reviews [59].

C3I for a cyber SIOP

C3I requirements for strategic OCO mirror some, though not all, of the requirements for nuclear operations. For nuclear operations the main requirements are "... that NC3 nuclear command, control, and communications must be reliable, assured, enduring, redundant, unambiguous, survivable, secure, timely, flexible, and accurate" [60]. In addition to C3, nuclear forces require an intelligence component for early warning, assessing incoming attacks (at a minimum to distinguish very large from very small attacks), and to perform postattack evaluation of both incoming strikes from adversaries and outgoing strikes [61].

The C3 requirements for OCO are the same as NC3 but perhaps not as stringent. For example, the survivability requirement for NC3 is extreme – a minimum warning nuclear attack by a major power. Unless OCO are a major component of US retaliatory capabilities for such an attack OCO C3 need not be as survivable as NC3. Moreover, the forces that execute OCO may not be nearly as survivable as some elements of US nuclear forces, making highly survivable C3 for OCO a poor investment.

As an example, the US Air Force planned to contribute 39 teams to the Cyber Mission Force (CMF) as of May 2014, of which 19 were teams that could have an OCO mission (the other 20 are Cyber Protection Teams). Those teams were allocated to just five bases (two of which are in the greater San Antonio area) [62]. A handful of nuclear strikes – and possibly even a robust conventional strike – could destroy or disable the entire Air Force contribution to OCO. In contrast, Air Force ICBMs, 450 of which are distributed in hardened silos, would require hundreds of nuclear weapons to destroy. In short, C3 need not be more survivable than the actual forces, whether nuclear or cyber. OCO forces may be significantly more vulnerable than nuclear forces, so C3 need not be that survivable.

On the other hand, the C2 issues associated with OCO forces assigned to regional combatant commanders noted earlier create issues for the overall OCO C3 structure. If OCO forces assigned to a regional combatant commander are not collocated with the command headquarters, C3 must be sufficiently survivable to prevent the easy severing of combatant commanders from OCO forces. Only two of the Air Force teams potentially capable of OCO were planned to be located outside the continental USA (in this case in Hawaii, where Pacific Command is headquartered). The other teams, in Texas and Georgia, could be assigned to support distant commands, such as European Command (EUCOM), making them highly reliant on classified communications systems.

If C3 for OCO is based on the standard Department of Defense protocol for Top Secret/Sensitive Compartmented Information (TS/SCI), it may not meet this standard of survivability (on TS/SCI IP, see [63]). First, Department of Defense TS/SCI networks rely heavily on Defense Intelligence Agency (DIA) Regional Support Centers, of which there were only five in 2004 according to unclassified sources [64]. A relatively finite number of conventional strikes could therefore not only significantly damage US OCO forces but also the C3 allowing distant combatant commanders to effectively communicate with them.

Second, even short of conventional strikes on the USA, C3 may be vulnerable to adversary attack. Recent media reports have highlighted Russian efforts to map, and potentially target, undersea military communications cables in the Atlantic [65]. Severing these cables would greatly degrade but not eliminate C3 on networks linking EUCOM to US-based cyber forces. Satellite communications can provide a substitute, albeit at a lower data rate, for the cables.

However, Russia (and China) are both reported to be developing a wide array of abilities to target US space assets, including communications satellites. These include direct kinetic attack (anti-satellite missiles), electromagnetic (jamming satellite links), and even adversary OCO [66]. A combination of severing trans-Atlantic cables with even limited attacks on communications satellites could seriously impair OCO C3 from EUCOM without striking any ground targets (this same logic holds even if C3 is conducted over other classified networks such as the National Security Agency's NSANet).

Vulnerability of C3 in the nuclear realm led to significant concerns about strategic stability, as it created incentives for preemptive attack. Preemption, by disrupting C3, could yield significant military benefits, which in turn made crises less stable – the nuclear equivalent of the World War I mobilization mania [5,67]. Similar vulnerability of C3 for OCO, combined with the potential vulnerability of OCO forces themselves, may create crisis instability as one or both sides could perceive utility in preemptive attack.

Yet the utility of preemption may be more limited, as cable-based communication within the USA may be less vulnerable than trans-Atlantic cables. OCO forces based in the USA could thus be directed by Cyber Command (CYBERCOM)/STRATCOM rather than EUCOM, a less efficient C3 arrangement perhaps but better than nothing. Yet the severing of links between Europe and the USA could degrade access to some targets for OCO even if C3 is maintained.

The intelligence requirements for OCO are difficult but better understood in some ways. Early warning of adversary OCO is well appreciated as a critical but difficult component of cyber defense. For example, the US Intelligence Advanced Research Projects Agency (IARPA) is seeking to invest in novel means for cyber early warning [68].

Potentially more challenging is the ability to assess the effectiveness of OCO. Briefing a group of pilots about to conduct airstrikes that despite imagery showing an intact air defense system it is ok to proceed, because OCO has disabled missiles and radars would be challenging to say the least. What if the adversary has created a false image of effective OCO in order to lure aircraft into an ambush?

Given this potential for deception by adversary defense cyber operations, assessing the effectiveness of OCO probably requires a "dual phenomenology" approach [32]. This would mean after initial indications of successful OCO from OCO forces, another intelligence collection platform would confirm the result. In the case of the Suter program, the results of the introduction of malware are reported to be independently assessed by US electronic warfare aircraft such as the RC-135 Rivet Joint [52].

Similar intelligence collection may be required to verify the efficacy of other types of OCO. For example, OCO against targets with visual signatures (e.g. an electric power grid) could be verified by overhead imagery. Much more difficult would be verifying OCO against regime internal security databases, though perhaps communications intelligence (COMINT) might detect adversary discussions of the attack, though this too could be part of a deception operation.

Theater and strategic OCO: a blurry firebreak

One of the central distinctions in the nuclear era was between theater nuclear forces (and operations) and strategic nuclear forces. The SIOP was developed to govern strategic forces while theater forces were governed by the relevant theater commanders. The Supreme Allied Commander Europe (SACEUR), the American general commanding NATO forces, had a plan for the coordinated delivery of NATO theater nuclear forces. Below SACEUR's level, various tactical commanders could potentially be authorized to use nuclear weapons for relatively limited tactical effects [69].

Over time US leaders became increasingly uncomfortable with tactical commanders having delegated authority to use nuclear weapons. The potential for escalation and other strategic effects from tactical nuclear use combined with a general decision by the US Army to refocus on conventional military operations after 1960 limited the development of very serious thinking about tactical nuclear use. Yet the boundary between theater and strategic was often opaque or arbitrary. For example, one of the long-standing distinctions in plans was geographic, with SACEUR's plans from the 1960s onward limited to NATO and Warsaw Pact territory outside the Soviet Union, while the SIOP would handle targets inside the Soviet Union. Yet this distinction began to blur as longer range theater forces, such as the Pershing II intermediate range ballistic missile and Gryphon ground launched cruise missile, were deployed in the early 1980s [69,70].

OCO, in contrast to nuclear operations, have long been viewed as primarily (though not exclusively) strategic. While US regional combatant commanders have long had an information operations capability that includes electronic warfare, military deception, and special technical operations and is thus capable of some OCO (or OCO-like) functions, the remit for such operations remains limited. Indeed, relatively early in the development of OCO the joint task force charged with such operations was placed under US STRATCOM. When that organization evolved into US CYBERCOM it remained a sub-unified command under STRATCOM. At present the authorization for OCO, like nuclear operations, remains with the US NCA (i.e. the President and

Secretary of Defense) (see remarks by Vice Chief of Naval Operations Admiral Michelle Howard in [71]; [72]).

Yet the trajectories of the two types of operations may be radically different. While nuclear operations became increasingly centralized in the early decades of the nuclear age, OCO are beginning to decentralize. The current plan for a CMF envisions a number of Combat Mission Forces that "... will support combatant commands by generating integrated cyberspace effects in support of operational plans and contingency operations." This presumably could include OCO for theater purposes. CYBERCOM will retain a National Mission Force, which will likewise presumably conduct strategic OCO [73].

As a series of war games and reports have noted, the existence of theater cyber forces will require a change in C2 and potentially a willingness to delegate authority to conduct OCO to commanders below the NCA level [74,75]. In terms of C2, many analysts agree theater cyber forces should fall under a cyber (or information) component commander. This C2 architecture would parallel the special operations model, where each regional commander has a theater special operations command (TSOC), which is organized by US Special Operations Command but operationally controlled by the regional commander.

Yet C2 organization without authorities to both prepare for and also execute theater level OCO will not produce a meaningful capability. As subsequent sections describe, there are real limits on the ability to effectively plan and target OCO absent extensive intelligence collection and target development. However, the risks of inadvertent escalation leaders worried about with theater nuclear operations are at least as prominent with theater OCO. Leaders may be unwilling to delegate authorities necessary for theater OCO, limiting the utility of theater cyber forces regardless of C2 architecture.

At the same time, some capabilities that strongly resemble OCO may be included as a subset of more traditional elements of theater forces. For example, electronic warfare, the use of the electromagnetic spectrum for offensive or defensive purposes, is a standard element of a regional combatant commander's forces. Yet sophisticated electronic warfare programs use the generation of false signals and in some cases introduction of malware.

The boundary between electronic warfare and OCO may be clearer at the classified level but it merits significant consideration. If programs like Suter are considered OCO, then they will likely require authorization by the NCA, which may in turn reduce the effort regional combatant commanders expend on incorporating them fully into their operational plans. Why rely on a capability requiring authorization that may not be forthcoming in a conflict? Alternately if Suter and similar systems are simply a form of electronic warfare, policymakers may be unpleasantly surprised to discover their use in a conflict without NCA-level authorization. These operational boundaries should be carefully delineated as part of the development of regional cyber C2.

The future of strategic OCO

The next US administration will have to grapple with all of the foregoing operational considerations for OCO. It should therefore pursue a Cyber Posture Review in parallel to other strategic reviews, such as the Nuclear Posture Review and the Ballistic Missile Defense Review. This review would provide the critical guidance for OCO targeting development and C3I noted above.

For an administration seeking to capitalize on USA strengths in OCO, this review might generate guidance that assumes escalation risk by seeking to develop options against critical adversary assets such as national and nuclear C2. In contrast, an administration concerned about the potential for inadvertent escalation from seeking to develop access to critical C2 might impose strict targeting limits on OCO, such as greatly confined regional scope for such operations.

Similarly, the next administration may embrace an OCO posture focusing on deterrence by punishment through countervalue retaliation. It might also impose damage expectancy focusing on destruction rather than disruption. Alternately it may eschew countervalue OCO in favor of counterforce targeting, emphasizing disrupting adversary OCO C3 and force structure in order to prevail in a short but sharp conventional conflict.

Central to any future for strategic OCO is a vision of the role of OCO in the broader US defense strategy. At the time the nuclear SIOP was developed, US strategic nuclear forces were the force of last resort and the lynchpin of US extended deterrence [76]. After the end of the Cold War, nuclear weapons became less central to US military posture and the SIOP was officially retired in 2003, replaced by other operational plans [77]. In contrast, the role of cyber SIOP in US military posture is just beginning.

References

1. Long A. *Deterrence from Cold War to Long War: Lessons from Six Decades of RAND Research*. Santa Monica: RAND Corporation, 2008, 28–31.
2. Nolan J. *Guardians of the Arsenal: The Politics of Nuclear Strategy*. New York: Basic Books, 1989.
3. Miller F. Masters of the nuclear weapons enterprise. In: Butler, G. (ed.), *Uncommon Cause: A Life at Odds with Convention*, vol. **2**. Parker: Outskirts Press, 2016.
4. Trachtenberg M. Strategic thought in America, 1952–1966. *Polit Sci Q* 1989;**104**:301–34.
5. Steinbruner J. National security and the concept of strategic stability. *J Confl Resolut* 1978;**22**:411–28.
6. Carter A, Steinbruner J, Zraket C. *Managing Nuclear Operations*. Washington, DC: Brookings Institutions, 1987.
7. Eden L, Miller S, Sullivan D, *et al*. *Nuclear Arguments: The Major Debates on Strategic Nuclear Weapons and Arms Control*. Ithaca: Cornell University Press, 1989.
8. Clarke R, Knake R. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2010.
9. Brenner J. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin, 2011.
10. Kello L. The meaning of the cyber revolution: perils to theory and statecraft. *Int Security* 2013;**38**:7–40.
11. Kaspersky Lab. Equation Group: Questions and Answers, 2015 https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf (last accessed January 30, 2017).
12. Synder GH. *Deterrence and Defense: Toward a Theory of National Security*. Princeton: Princeton University Press, 1961.
13. Ball D and Richelson J (eds). *Strategic Nuclear Targeting*. Ithaca: Cornell University Press, 1986.
14. Kristensen H. *The U.S. Nuclear Posture After the 2010 Nuclear Posture Review and 2013 Nuclear Employment Strategy*, Federation of American Scientists, 2013. https://fas.org/programs/ssp/nukes/publications1/Brief2013_Georgetown.pdf (2 December 2016, date last accessed).
15. Greenwald G, MacAskill E. Obama orders US to draw up overseas target list for cyber-attacks. *The Guardian*. https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas (2 December 2016, date last accessed).
16. Policy Guidance for the Employment of Nuclear Weapons. http://nsarchive.gwu.edu/NSAEBB/NSAEBB173/SIOP-25.pdf (23 October 2016, date last accessed).
17. Fact Sheet: Nuclear Weapons Employment Strategy of the United States. https://www.whitehouse.gov/the-press-office/2013/06/19/fact-sheet-nuclear-weapons-employment-strategy-united-states (17 September 2016, date last accessed).

18. Posen B. *Inadvertent Escalation: Conventional War and Nuclear Risks*. Ithaca: Cornell University Press, 1991.
19. Rovner J. AirSea battle and escalation risks. University of California Institute on Global Conflict and Cooperation, 2012, 1–5.
20. Talmadge C. Assessing the risk of Chinese nuclear escalation in a conventional war with the United States. Draft manuscript, 2016.
21. Kulesa Ł. *Towards a New Equilibrium: Minimising The Risks of NATO and Russia's New Military Postures*. European Leadership Network. http://www.europeanleadershipnetwork.org/medialibrary/2016/02/07/180d69f6/Towards%20a%20New%20Equilibrium%202016.pdf (2 December 2016, data last accessed).
22. Blair B. *The Logic of Accidental Nuclear War*. Washington, DC: Brookings Institution Press, 1993, 127–28.
23. Harvey J. Commentary: negating North Korea's nukes. *Defense News*. http://www.defensenews.com/story/defense/commentary/2016/02/15/commentary-negating-north-koreas-nukes/80189872/ (2 December 2016, date last accessed).
24. Lindsay J. Stuxnet and the limits of cyberwarfare. *Secur Stud* 2013;**22**:365–404.
25. Mandiant. *APT1: Exposing One of China's Cyber Espionage Units*. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (2 December 2016, date last accessed).
26. Fischer B. CANOPY WING: the U.S. war plan that gave the East Germans goose bumps. *Int J Intell Counterintell* 2014;**27**:431–64.
27. Kaplan F. *Dark Territory: The Secret History of Cyber War*. New York: Simon and Schuster, 2016, 12–20.
28. Richards J. Denial-of-Service: the Estonian cyberwar and its implications for U.S. national security. George Washington University International Affairs Review 2009, 18.
29. Healey, J (ed.). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Washington, DC: Cyber Conflict Studies Association, 2013.
30. Assante M, Conway T, Lee R. *German Steel Mill Cyber Attack*, SANS Industrial Control System, 2014. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf (2 December 2016, date last accessed).
31. Kelley M. The Sony hack wrecked a lot of equipment. *Business Insider*. http://www.businessinsider.com/we-now-have-an-idea-of-the-sony-hacks-destruction-2015-1 (2 December 2016, date last accessed).
32. Gartzke E, Lindsay J. Weaving tangled webs: offense, defense, and deception in cyberspace. *Secur Stud* 2015;**24**:316–48.
33. Official U.S. Government information about the Global Positioning System (GPS) and related topics. http://www.gps.gov/systems/gps/control/ (2 December 2016, date last accessed).
34. Edelman B, Zittrain J. *Empirical Analysis of Internet Filtering in China*. Berkman Center for Internet & Society. http://cyber.law.harvard.edu/filtering/china/appendix-tech.html (2 December 2016, date last accessed).
35. Dougherty R. The psychological climate of nuclear command. In: Carter A, Steinbruner J, Zraket C (eds), *Managing Nuclear Operations*. Washington DC: Brookings Institution, 1987, 412.
36. Richelson J. Dilemmas in counterpower targeting. *Comp Strateg* 1980;**2**:164–165.
37. Lin, H. Offensive cyber operations and the use of force. *J Natl Sec L Poly* 2010;**4**:63–86.
38. Conversation with Senior Adviser to U.S. Cyber Command, March 2016.
39. Hsu J. *Why the NSA's Spying on Offline Computers Is Less Scary Than Mass Surveillance*. IEEE Spectrum. http://spectrum.ieee.org/tech-talk/telecom/wireless/why-the-nsa-spying-on-offline-computers-is-less-scary-than-mass-surveillance (2 December 2016, date last accessed).
40. Freedberg S. *Wireless Hacking in Flight: Air Force Demos Cyber EC-130*. Breaking Defense. http://breakingdefense.com/2015/09/wireless-hacking-in-flight-air-force-demos-cyber-ec-130/ (18 January 2017, date last accessed).
41. Shapiro B. Acquire, Assess, Exploit. *Airman Magazine*, 21 November 2016 http://www.nasic.af.mil/News/ArticleDisplay/tabid/1356/Article/1010245/acquire-assess-exploit.aspx (18 January 2017, date last accessed).
42. Barron J. *MiG Pilot: The Final Escape of Lieutenant Belenko*. New York: McGraw-Hill, 1980.
43. Hoffman D. *The Billion Dollar Spy: A True Story of Cold War Espionage and Betrayal*. New York: Doubleday, 2015.
44. Fischer B. The spy who came in for the gold: a skeptical view of the GTVANQUISH case. *J Intell Hist* 2008;**8**:29–54.
45. Topol-M. Jane's Strategic Weapons Systems, 2 November 2016.
46. Lieber K. *War and the Engineers: The Primacy of Politics over Technology*. Ithaca: Cornell University Press, 2005.
47. Biddle S. Rebuilding the foundations of offense-defense theory. *J Polit* 2001;**63**:741–74.
48. Rid T. Cyber war will not take place. *J Strateg Stud* 2012;**35**:5–32.
49. Compass Call. Jane's C4ISR & Mission Systems: Air, 17 May 2016.
50. Defense Science Board Task Force. *Resilient Military Systems and the Advanced Cyber Threat*. *Defense Science Board* 2013.
51. Chaim K, Glaser C. What is the offense-defense balance and can we measure it? *Intl Security* 1998;**22**:46.
52. Gasparre R. *The Israeli 'E-tack' on Syria – Part II*. Air Force Technology. http://www.airforce-technology.com/features/feature1669/ (2 December 2016, date last accessed).
53. USAF Project Suter Briefing (n.d.).
54. Schmitt E, Shanker T. U.S. debated cyberwarfare in attack plan on Libya. *New York Times*. http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html (2 December 2016, date last accessed).
55. Fulghum D, China US. Chase air-to-air cyber weapon. *Aviation Week*. http://aviationweek.com/defense/china-us-chase-air-air-cyber-weapon (2 December 2016, date last accessed).
56. Finkle J. Bangladesh bank hackers compromised SWIFT software, warning issued. *Reuters*. http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR (2 December 2016, date last accessed).
57. USSTRATCOM Global Operations Center Fact Sheet. https://www.stratcom.mil/factsheets/3/Global_Operations_Center/printable/ (2 December 2016, date last accessed).
58. Anderlini J, Mitchell T. Top China defector passes secrets to U.S. *Financial Times*. https://www.ft.com/content/4e900936-cb20-11e5-a8ef-ea66e967dd44 (2 December 2016, date last accessed).
59. Ball D. The development of the SIOP, 1960-1983. In: Ball D, Jeffrey R (eds), *Strategic Nuclear Targeting*. Ithaca: Cornell University Press, 1986.
60. Nuclear Matters Handbook. Department of Defense. http://www.acq.osd.mil/ncbdp/nm/NMHB/chapters/chapter_6.htm (2 December 2016, date last accessed).
61. Toomay J. Warning and assessment sensors. In: Carter A, Steinbruner J, Zraket C (eds), *Managing Nuclear Operations*. Washington DC: Brookings Institution, 1987.
62. USCYBERCOMMAND Cyber Mission Force. *U.S. Air Force*. http://www.safcioa6.af.mil/shared/media/document/AFD-140512-039.pdf (2 December 2016, date last accessed).
63. TS/SCI IP Data. *Defense Information Systems Agency*. http://www.disa.mil/Network-Services/Data/TS-SCI-IP (2 December 2016, date last accessed).
64. Communique. *Defense Intelligence Agency Publication* 2004, 16:4. https://issuu.com/nationalsecurityarchive/docs/communique-2004-december (2 December 2016, date last accessed).
65. Sanger D, Schmitt E. Russian ships near data cables are too close for U.S. comfort. *New York Times*. https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0 (2 December 2016, date last accessed).
66. Colby E. *From Sanctuary to Battlefield: A Framework for a U.S. Defense and Deterrence Strategy for Space*. Washington, DC: Center for New American Security, 2016.
67. Snyder J. *The Ideology of the Offensive: Military Decision-Making and the Disasters of 1914*. Ithaca: Cornell University Press, 1984.
68. McCaney K. IARPA wants an early warning system for Cyber Attacks. *Defense Systems*. https://defensesystems.com/articles/2015/07/24/iarpa-cause-cyber-early-warning-system.aspx (2 December 2016, date last accessed).
69. Kelleher, C. NATO nuclear operations. In Carter A, Steinbruner J, Zraket C (eds), *Managing Nuclear Operations*. Washington DC: Brookings Institution, 1987.

70. Postol T. Targeting. In Carter A, Steinbruner J, Zraket C (eds), *Managing Nuclear Operations*. Washington DC: Brookings Institution, 1987.
71. Maucione S. Cyber offensive weapons pits strategic vs. tactical. *Federal News Radio*. http://federalnewsradio.com/defense/2015/09/top-naval-official-will-take-presidents-permission-use-offensive-cyber-weapon/ (2 December 2016, date last accessed).
72. Lewis J. The role of offensive cyber operations in NATO's collective defence. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper No. 8, 2015.
73. Department of Defense Cyber Strategy. Department of Defense. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (2 December 2016, date last accessed).
74. Naval War College Report Reveals New Joint Defense Needs. Naval War College Public Affairs. http://www.navy.mil/submit/display.asp?story_id=85958 (2 December 2016, date last accessed).
75. FitzGerald B, Wright P. *Digital Theaters: Decentralizing Cyber Command and Control*. Washington, DC: Center for New American Security, 2014.
76. Ravenal E. Counterforce and alliance: the ultimate connection. *Intl Security* 1982;**6**:26–43.
77. Kristensen H. Obama and the Nuclear War Plan. *Federation of American Scientists*, 2010. https://fas.org/programs/ssp/nukes/publications1/WarPlanIssueBrief2010.pdf (2 December 2016, date last accessed).