May 19, 2010

Traditional Military Activities in Cyberspace: Preparing for "Netwar"

Paul A. Walker

Traditional Military Activities in Cyberspace: Preparing For "Netwar"

By Paul A. Walker

Abstract: Recently, questions have arisen regarding the U.S. military's actions in cyberspace with some claiming those activities fall under the covert action reporting statute. This Article examines this questions and concludes that such actions are not subject to the covert action reporting statute because they are traditional military activities, an exemption provided by Congress when the covert action reporting statute was passed as part of the Intelligence Authorization Act of 1991. An examination of the legislative history reveals wide latitude for military operations that are conducted under the "direction and control" of a military commander prior to, or during, anticipated hostilities. In fact, the legislative history goes so far as to provide that such activities do not have to be apparent or acknowledged. The Article then goes on to conduct a historical examination of military activity that contributes to strategic surprise in order to analogize to similar activities that could occur in cyberspace. The Article concludes that most such activities may be conducted by the U.S. military without triggering the covert action reporting requirement.

The United States government recently launched a "cyberattack" on itself. According to a report in the *Washington Post*, the Department of Defense (DoD) "mounted a cyberattack that dismantled [an] online forum" that was apparently "set up" by the Central Intelligence Agency (CIA).[1] The web site was used by the CIA, along with its Saudi Arabian counterpart, to monitor ongoing terrorist activity in the Saudi kingdom.[2] Military commanders viewed the web site as a threat because it was being used by terrorists to exchange operational information and plan attacks on soldiers in the United States Central Command area of operations.[3] Following lengthy briefings and discussions of legal authority, and over a vigorous dissent from the CIA, a high-level task force apparently gave approval for the military to conduct the cyber action against the

[1] Ellen Nakashima, *Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies*, THE WASHINGTON POST, Mar. 19, 2010, at A1.
[2] *Id*.
[3] *Id*.

extremist website.[4] According to the article, the action was carried out by the Joint Functional Component Command-Network Warfare, based at Fort Meade, Maryland.[5]

The *Post* article raises a number of legal and policy issues highlighted by this episode. The article raises a broad point regarding the legal authority for the military to carry out such activities. This concern is alleged against the backdrop of an apparently ongoing dispute between the CIA and the active duty military over whether such an action is a "covert action" or a "traditional military activity."[6] The most tangible result of such a dispute is whether or not the cyber action carried out by the military has to be reported to Congress in accordance with the covert action oversight statute, 50 U.S.C. § 413b. The broader result, of course, is about control; not only about who does such activities, but control over the activities themselves. Previously, the same kind of inter-agency dispute erupted over the use of Special Operations forces in activities that, if carried out by the CIA, could be considered "covert action."[7]

These legal and policy disputes over the employment of Special Operations forces and information-based actions, such as the attack on the jihadist web-site, will grow increasingly important in the coming years. The United States faces an agile, networked adversary. The age

---

[4] *Id*.

[5] *Id*. The article refers a number of times to the National Security Agency (NSA) and its Director, Lieutenant General Keith B. Alexander. To the extent the article may give the impression that Lieutenant General Alexander and NSA were in the line of command for the alleged "cyberattack," such an impression would be mistaken. The JFCC-Network Warfare is actually a component command of the United States Strategic Command, which is currently under the command of General Kevin P. Chilton. *See* United States Strategic Command Factsheet, available at http://www.stratcom.mil/factsheets/snapshot/.

[6] Nakashima, *supra* note 1, at A1("The use of computers to gather intelligence or to disrupt the enemy presents complex questions: When is a cyberattack outside the theater of war allowed? Is taking out an extremist Web site a covert operation or a traditional military activity? Should Congress be informed?").

[7] *See, e.g.*, Richard C. Gross, *Different Worlds: Unacknowledged Special Operations and Covert Action*, Strategy Research Paper, U.S. Army War College, Mar. 30, 2009, at 2 (discussing the ongoing "debate about the blurred operational lines between the CIA on one hand and DoD special operations forces hunting terrorists worldwide on the other"). *See also* Jennifer D. Kibbe, *The Rise of the Shadow Warriors*, Foreign Affairs, Mar.-Apr. 2004 (arguing that military special operations often amount to the functional equivalent of "covert action" and should be held to the same standard of accountability as CIA covert actions); Seymour M. Hersh, *The Coming Wars: What the Pentagon Can Now Do in Secret*, THE NEW YORKER, Jan. 24, 2005, (discussing then-Secretary of Defense Rumsfeld's use of Special Forces units in covert action).

of "netwar" is upon us.[8] Speed and flexibility will be essential to meeting and defeating networked enemies, such as al Qaeda. John Arquilla, the foremost thinker about networked warfare, recently called for the military to develop new rules for confronting such enemies.[9] In a nutshell, Arquilla's rules are: "Many and small" forces finding rather than flanking the adversary by swarming, not surging.[10] Special Operations forces are in the forefront of today's military in this style of warfare. Special Operations units are normally broken down into twelve-man "A teams" or squads, depending on the service.[11] The teams train as a unit and are often called on to carry out operations that would require greater numbers of regular troops.[12] Likewise, information-based warfare assumes greater prominence and dominance in a world dominated by networks. Warfare using the network of networks—the Internet—will be the ultimate force multiplier against networked adversaries, whether they are international terrorists, international drug traffickers or the armed forces of adversary states. In order to respond with the speed and agility required in a networked environment, legal rules and authorities must keep pace with technology and changing methods of warfare.

The first step in achieving this speed and agility is recognizing that there are a vast array of traditional military activities that can occur in the internet and other information environments that do not need to be reported to Congress as "covert actions." Although one may argue with it

[8] The term "netwar" was coined by Rand researchers John Arquilla and David Ronfeldt and refers to conflicts waged by terrorists, criminals, gangs, ethnic extremists, and civil-society activists that use a networked organizational structure and make it critical that government, the military and law enforcement begin networking themselves. *See* NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME AND MILITANCY ix (John Arquilla & David Ronfeldt eds., 2001).

[9] John Arquilla, *The New Rules of War*, FOREIGN POLICY, Mar.-Apr. 2010.

[10] *Id*. The actual rules Arquilla sets forth are: "Rule 1: 'Many and Small' Beats 'Few and Large'", "Rule 2: Finding Matters More Than Flanking," and "Rule 3: Swarming is the New Surging."

[11] *See* ROBIN NEILLANDS, IN THE COMBAT ZONE: SPECIAL FORCES SINCE 1945 164 (1998).

[12] *See id*. at 46 (quoting a World War II [British] Commando officer as telling his men "Given time, any infantry unit can do what we do; the point is that only Commandos can do it in the time available.").

as a policy decision,[13] this article argues that the military's decision to conduct a cyber action against the CIA/Saudi-monitored web site was well within the norms of traditional military activity. Because the action occurred during the course of an armed conflict against al Qaeda, there would also be no need to acknowledge such an action when it was directed by a military commander. The article explores the array of traditional military activities that may occur in the internet and other information environments without triggering covert action reporting requirements through the prism of a historical examination of two types of military activity that contribute to the accomplishment of strategic surprise: positioning of forces and deception operations.

Part I of the article examines the language and legislative history of the definition of "covert action." The legislative history is particularly important to understanding this definition, which is unfortunate given the often cursory treatment it has received in the academic literature.[14] The legislative history draws some clear boundaries that need to be explored in order to provide the proper context for the subsequent discussion. Part II of the article examines the historical use of two types of military activity, force positioning and deception operation, in accomplishing strategic surprise. This examination occurs in parallel with an examination of analogous hypothetical and not-so hypothetical information-based actions occurring within and against the Internet and other information-based networks and equipment. The latter sections also examine

[13] In essence, this appears to be a variant of the classic tension that occurs between law enforcement and counter-intelligence. Here, though, the tension is not between continued intelligence collection and prosecution, but between collection and elimination of operational threats. As Martin Libicki explains, in the context of "cyberwar," "[i]ntelligence operatives are oriented toward finding information about the adversary. Military operators are oriented toward reducing the adversary's ability to wage war, which in this context, generally means reducing the its (sic) ability to take advantage of information and communications." MARTIN LIBICKI, CYBERDETERRENCE AND CYBERWAR 155-56 (2009).

[14] *See* Joel T. Meyer, *Recent Developments: Supervising the Pentagon: Covert Action and Traditional Military Activities in the War on Terror*, 59 ADMIN. L. REV. 463, --- (2007) (citing conference and Senate report from the pocket-vetoed 1990 Intelligence Authorization Act rather than the reports that accompanied the Act that passed the following year); Michael McAndrew, *Note*, *Wrangling In The Shadows: The Use Of United States Special Forces In Covert Military Operations In The War On Terror*, 29 B.C Int'l & Comp. L. Rev. 153, 154-55 (2006) (spending less than a paragraph on the legislative history).

and discuss why these information-based actions fit within the rubric of "traditional military activities." Finally, Part III concludes the article with an assessment of the applicability of traditional military activities in "cyberspace" and discusses the oversight mechanisms applicable to "traditional military activity." This section concludes that the same policy concerns requiring aggressive oversight of covert action are mitigated by the multi-layered review process inherent in the war planning process.

I. The Covert Action Reporting Statute

A. Defining "Covert Action"

Congress first defined "covert action" in 1991.[15] The Intelligence Authorization Act for that year added a section titled "Presidential Approval and Reporting of Covert Actions" to the National Security Act of 1947. In what was largely a codification of then-existing Executive practice,[16] the section required the President to issue, in writing, a "finding" authorizing any proposed covert action.[17] Congress also made it clear that, in making such a finding, the President had to determine that the covert action he was approving was "necessary to *support identifiable foreign policy objectives* of the United States and is important to the national security of the United States."[18] The new section also imposed a number of additional process requirements, such as detailing the specific requirements for written findings[19]; Congressional notification procedures, including notification of significant changes or additions based on

[15] The current definition in 50 U.S.C. §413b(e) is unchanged from this first enactment.
[16] *See generally* William E. Conner, *Reforming Oversight of Covert Actions After the Iran-Contra Affair: A Legislative History of the Intelligence Authorization Act for FY 1991*, 32 VA. J. INT'L L. 871, 902-918 (1992) (discussing the provisions of various National Security Decision Directives (NSDDs) issued by President Reagan in the wake of the Iran-Contra affair that instituted additional process requirements for covert actions). Conner later concludes that "the Act's notification requirements do not radically depart from existing covert action reporting procedures which were promulgated previously by various Executive Orders and NSDDs." *Id*. at 922.
[17] 50 U.S.C. §413b(a)(1).
[18] 50 U.S.C. §413b(a).
[19] 50 U.S.C. §413b(a)(3)-(5).

previously approved findings[20]; and an actual definition of "covert action." Subsection (e) defined "covert action" as "activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or publicly acknowledged."[21] This is the affirmative portion of the definition. This portion can be further broken down into purpose and methodology.

First, as to purpose, covert actions are used to influence conditions abroad, or outside the United States. According to the definition, that influence can be felt in three fairly broad areas: political, economic and military. Interestingly, neither the statute, nor the legislative history, provide specific guidance as to what constitutes "military conditions."[22] The legislative history does make it clear that the definition was meant to encompass then-existing practices.[23] The fairest reading, then, is that "military conditions" is meant to encompass the types of paramilitary operations carried out by the CIA, usually by arming and equipping indigenous or guerilla forces or by conducting "over the border" operations that cannot be carried out by United States military forces for political reasons. What must be understood, though, is that simply influencing conditions abroad is not sufficient to justify carrying out a covert action. Implicit in the requirements for a Presidential finding is the added purpose that the condition to be influenced by the covert action support an "identifiable foreign policy objective[] of the United

---

[20] 50 U.S.C. §413b(b)-(d).
[21] 50 U.S.C. §413b(e).
[22] The Conference Report, in the context of counterintelligence, does mention that such activities could cross a line into covert action if they are "undertaken to effect major changes in the national defense policies of such foreign powers or to provoke significant military responses by such foreign powers." H.R. Rep. No. 102-166 (1991) (Conf. Rep.). Interestingly, despite the seemingly obvious connection, this language is not tied to the statute's use of "military conditions," nor is it repeated in the portion of the report that discusses traditional military activities.
[23] The Conference Report stated:

> The conferees further note that in defining for the first time in statute the term "covert action" they do not intend that the new definition exclude any activity which heretofore has been understood to be a covert action, nor to include any activity not heretofore understood to be a covert action The new definition is meant to clarify the understanding of intelligence activities that require presidential approval and reporting to Congress; not to relax or go beyond previous understandings.

H.R. Rep. No. 102-166.

States." So, the *purpose of a covert action is to support identifiable foreign policy objectives of the United States by influencing political, economic, or military conditions abroad.* This linkage between covert action and broader United States foreign policy objectives is a distinction that assumes greater importance when the purpose of "traditional military activities" is later examined.

Whereas the first portion of the definition concerns *what* will be accomplished through covert action, the second portion concerns *how* the action will be accomplished. Covert actions are carried out in a manner such that either the role of the United States government is not apparent, or that role is not to be acknowledged. The use of the disjunctive "or" means that a covert action could occur where the role of the United States is not to be acknowledged, *even if* United States involvement is readily "apparent" in the results of effects of the covert action. The use of such "overt-covert actions"[24] increased during the Reagan and first Bush administrations and continues today. As a current example, it is widely reported that the CIA is operating the Predator drones carrying out airstrikes against al Qaeda leadership in Pakistan.[25] Initially, the mission was apparently entrusted to the CIA given the political sensitivities such strikes would cause for the Pakistani government.[26] Yet, despite widespread publicity, the United States has steadfastly refused to officially confirm the role of the CIA in these strikes, despite the suicide strike directed at CIA officers in Afghanistan allegedly involved in such strikes.[27] If true, this is the type of classic "over the border" covert action historically given to the CIA, for example in

---

[24] JEFFREY T. RICHELSON, THE U.S. INTELLIGENCE COMMUNITY 349 (4th ed. 1999). Richelson points to the efforts to overthrow the Sandinista government and support for the Afghan resistance to the Soviets as the "clearest" examples of "overt-covert example." *Id*.

[25] See, e.g., Scott Shane, CIA to Expand Use of Drones in Pakistan, N.Y. Times, Dec. 4, 2009, at A1 (calling the CIA-run program "[o]ne of Washington's worst-kept secrets"), available at http://www.nytimes.com/2009/12/04/world/asia/04drones.html?scp=1&sq=cia%20expanding%20drone%20assaults%20in%20pakistan&st=cse.

[26] *Id*.

[27] Joby Warrick & Pamela Constable, *Attacked CIA Facility Supported Drone Strikes*, Wash. Post, Jan. 1, 2010, at A1.

Cambodia during the Vietnam War. Unfortunately, there is often too much emphasis on this aspect of the definition, particularly in popular media accounts, without accounting for the fact that this portion works conjunctively with the purpose portion of the definition. As a result, popular accounts sweep too broadly, often characterizing actions as "covert" that are clearly not, merely because the activity is hidden from public view.

Another prominent feature of the definition is that it is neutral in application. In other words, it does not apply to any specific executive branch agency, for instance the CIA, but instead applies to the "United States Government" as a whole. A former National Security Council legal adviser, Judge James E. Baker, described the definition as "act-based, not actor-based."[28] Judge Baker also recognizes, however, that such a characterization may be undercut by the negative portion of the definition, in other words, that portion describing the exceptions to the general definition of covert action.[29] Although the exceptions themselves are stated in terms of activities, in each case the activity is primarily identified with a major executive branch agency. For instance, "traditional counterintelligence activities"[30] and "traditional law enforcement activities"[31] encompass the entirety of Federal Bureau of Investigation (FBI) operations. And, to the extent the FBI recently began collecting foreign intelligence, there is an exception for "activities the primary purpose of which is to acquire intelligence,"[32] which is also the exception that covers the collection activities of the rest of the intelligence community.[33] Likewise, the State Department and Department of Defense are the agencies primarily covered by the

[28] JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 151 (2007).
[29] *Id*. at 157 ("uniformed military operations have historically not been considered or treated as covert activities. Thus, even if the definition is act based, *the exception for "traditional military activities" may effectively remove clandestine military operations from its reach*.") (emphasis added).
[30] 50 U.S.C. §413b(e)(1).
[31] 50 U.S.C. §413b(e)(3).
[32] 50 U.S.C. §413b(e)(1).
[33] *See, e.g.*, Executive Order 12333, as amended (using the term "clandestine" to refer to certain intelligence collection activities of certain intelligence agencies, including the intelligence and counter-intelligence activities of the armed forces).

exception for "traditional diplomatic or military activities or routine support to such activities."[34] Thus, while in theory the definition of covert action applies to more agencies than just the CIA, in actual, practical application the two agencies, FBI and DoD, that conduct activities most similar in appearance (though not purpose) to covert actions are essentially excepted from the scope of the definition. This becomes even more apparent in the case of the Defense Department when the legislative history is fully considered.

B. Legislative History and the "Traditional Military Activity" Exception

The legislative history draws two distinct lines to help address whether an action or activity is a traditional military activity or a covert action. The first, and clearest, line is whether the activity is under the "direction and control of a United States military commander."[35] The second line appears to be temporally-based in that there may be a point "well in advance of a possible or eventual U.S. military operation"[36] where a military-led activity could constitute a covert action, as long as the activity would not be considered "routine support" to the eventual military operation. Each of these lines deserves to be considered in greater detail.

The first bright line the House and Senate conferees drew was that "traditional military activities" are always controlled by a military commander.[37] Simply put, no military commander means it is not a traditional military activity. Most significantly, the United States government sponsorship of any specific "traditional military activity" does not have to be apparent, or even later acknowledged, when the activity precedes and is related to anticipated or ongoing hostilities and where the "fact of the U.S. role in the overall operation is apparent or to

[34] 50 U.S.C. §413b(e)(2). Rather than use the direct quotation format of "traditional. . . military activities", this article will use "traditional military activities" to refer to this exception.
[35] H.R. Rep. No. 102-166. The same language is also contained in the Senate Report on the Intelligence Authorization Act for 1991. *See* S. Rep. No. 102-85 (1991).
[36] H.R. Rep. No. 102-166.
[37] H.R. Rep. No. 102-166 ("Activities that are not under the direction and control of a military commander should not be considered as `traditional military activities.'").

be acknowledged publicly."[38] In other words, even if an activity undertaken by the military looks like a "covert action" because, in part, U.S. sponsorship is not apparent or will not be acknowledged, as long as the activity is under the direction and control of a U.S. military commander and the United States involvement in the overall conflict is apparent or has been acknowledged, the activity is a traditional military activity, not covert action. Simply put: military commanders do not have to acknowledge or make apparent activities that they conduct during acknowledged hostilities, whether ongoing or anticipated.

As an illustration, recall the military action against the extremist web site discussed in the introduction to this article. The State Department Legal Adviser, Harold Koh, recently reaffirmed that the United States is in either a "war of self-defense or armed conflict" with al Qaeda.[39] Hostilities, in other words. During hostilities, a military commander apparently ordered an action taken against a web site that served as a recruiting and information site for al Qaeda and other extremists. As the *Washington Post* article points out, the action was requested by a senior military commander in Iraq, who made a compelling case that the web site led to the deaths of American soldiers. Thus, in openly acknowledged, ongoing hostilities with al Qaeda, the military commander's direction to take action against the extremist web site is a traditional military activity and U.S. involvement in the action against the site does not have to be apparent or ever even acknowledged.

In fact, the legislative history is so clear on this point that it seriously undermines Judge Baker's contention that the covert action definition is act-based rather than actor-based. The actor at issue, though, is not a federal agency, but an individual: a military commander. In cases of ongoing hostilities, the legislative history does not place any limit on the type of acts or

[38] *Id*.
[39] Harold H. Koh, Legal Adviser, United States Department of State, The Obama Administration and International Law, Keynote Speech at the Annual Meeting of the American Society of International Law (Mar. 24, 2010).

activity that can be brought within the rubric of "traditional military activity." All that matters in such instances is that the activity is under the "direction and control of a military commander."[40]

Hostilities do not even have to be "ongoing" or even imminent, just "anticipated." The Conference Report defines hostilities that are "anticipated" as "meaning approval has been given by the National Command Authorities for the activities and for operational planning for hostilities."[41] Although the definition contemplates two separate approvals, one for the specific activity and another for the operational planning the activity supports, there is potentially broad application. Militaries routinely conduct "operational planning for hostilities." Colloquially, they are known as "war plans." Such operational planning often occurs years, even decades, before any actual hostilities.

For instance, before World War I, the German General Staff continually updated plans for future operations against France. The "Schlieffen Plan" was first developed beginning in 1895[42] and was extensively war-gamed in 1904-05.[43] Schlieffen's plan envisioned a massive flanking maneuver through Belgium, with only a small defensive force on the border opposite France.[44] The plan was continually updated and modified by his successors, in part because of French familiarity with the major outlines of the plan.[45] The plan actually employed by the Germans in 1914 shifted a significant number of divisions away from the flanking maneuver, placing them in defensive positions to the south.[46] Likewise, during the Cold War, the North Atlantic Treaty Organization (NATO) countries and Warsaw Pact countries both drew up extensive plans for land war in Europe, with NATO long anticipating a Soviet attack along the NATO central

---

[40] H.R. Rep. No. 102-166.
[41] *Id*.
[42] Klaus Knorr, *Strategic Surprise in Four European Wars*, in STRATEGIC MILITARY SURPRISE 16 (Klaus Knorr & Patrick Morgan, eds. 1983).
[43] *See* Stefan T. Possony, Translator's Comment, in WALDEMAR ERFURTH, SURPRISE 3, 9 (1943).
[44] Knorr, *supra* note 42, at 16.
[45] *Id*. at 17.
[46] *Id*. at 16.

front.[47] As part of the preparations for war with the Soviets, U.S. Special Forces were "charged with exploring the mountains of southern Germany and Austria, finding sites for guerilla bases, establishing dumps of weapons and explosives, and assisting the newly established German and Austrian Armies in clandestine and behind-the-lines operations."[48]

The actor-based distinction applies even when activities occur in anticipation of hostilities. When under the direction and control of a military commander, such activities do not have to be apparent or acknowledged, as long as U.S. involvement in the future hostilities will be later apparent or acknowledged. Even after U.S. involvement in hostilities is apparent or acknowledged, there would still be no requirement to acknowledge any of the "traditional military activities" that occurred in anticipation of the hostilities.

The Conference Report does attempt to place an ill-defined limit on "traditional military activities" in anticipation of hostilities. The Conferees stated: "Whether or not activities undertaken *well in advance* of a possible or eventual U.S. military operation constitute `covert action' will depend in most cases upon whether they constitute `routine support' to such an operation, as explained in the report accompanying the Senate bill."[49] The Conferees gave no indication of the temporal scope of "well in advance," so there is ambiguity as to where in time the line is between "routine support" and "traditional military activity." Put another way, where is the line between act-based determinations that an activity is a covert action and the actor-based

[47] *See* RICHARD K. BETTS, SURPRISE ATTACK 154 n.1 (1982) (defining the central front as "run[ning] from the Baltic, along the intra-German and Czechoslovakian borders, to the Austrian frontier"). Chapter Six of Betts's book analyzes the possibilities of strategic surprise by the Soviets in this area, and the factors that made NATO potentially vulnerable to such an attack. *Id*. at 153-88.

[48] ROBIN NEILLANDS, IN THE COMBAT ZONE: SPECIAL FORCES SINCE 1945 76 (1998) (describing the mission of the first post-war Special Forces unit, the 10th Special Forces Group).

[49] H.R. Rep. No. 102-166. The Senate report includes the sentence quoted in the text, but just before that sentence, the Senate is even more unambiguous on the point that unacknowledged military operations abroad in support of planning are traditional military activities: "The Committee also recognizes that even in the absence of anticipated or ongoing hostilities involving U.S. military forces there could potentially be requirements to conduct activities abroad which are not acknowledged by the United States to support the planning and execution of a military operation should it become necessary." S. Rep. No. 102-85.

"traditional military activity"? The Senate Report attempted to provide some guidance as to *what* was considered routine support, but provided no better idea as to *when* in the planning process "routine support" gives way to "traditional military activity."

In the Senate report, the unilateral nature of an activity is the lynchpin between "routine support" "well in advance" of a U.S. military operation and "other-than-routine" support. In the case of "routine support," the unilateral U.S. activity must relate to "logistical or other support for U.S. military forces in the event of a military operation that is to be publicly acknowledged."[50] Examples provided include "caching communications equipment or weapons, the lease or purchase from unwitting sources of residential or commercial property to support an aspect of an operation, or obtaining currency or documentation for possible operational uses, if the operation as a whole is to be publicly acknowledged."[51] Not all of the examples involve the U.S. military acting alone. But in those examples the "unwitting" third-party is carrying out a commercial transaction as he would with any other customer; he has not become an active part of the activity.

By way of contrast, the foreign nationals that appear in the Senate examples of "other-than-routine" support know they are dealing with the U.S. military and are actively participating in the activity:

> clandestine attempts to recruit or train foreign nationals with access to the target country to support U.S. forces in the event of a military operation; clandestine effects to influence foreign nationals of the target country concerned to take certain actions in the event of a U.S. military operation; clandestine efforts to influence and effect public opinion in the country concerned where U.S. sponsorship of such efforts is concealed; and clandestine efforts to influence foreign officials in third countries to take certain actions without the knowledge or approval of their government in the event of a U.S. military operation.[52]

[50] *Id*.
[51] *Id*.
[52] *Id*.

The last three examples use the word "influence," specifically tying those examples to the affirmative portion of the covert action definition. While the first example does not use "influence," it appears to be directed at the "military conditions" inside a target country, rather than the gathering of intelligence.[53] The Senate report considers these examples, where there is the active involvement of a foreign national in the U.S. military activity to be "other than unilateral" and thus "other-than-routine" support activities.

Taken as a whole, then, during the "well in advance" of hostilities timeframe, the key distinction for routine and non-routine support is for the U.S. military to act without actively involving foreign nationals to exert influence. There remain a great many logistical and support activities that can be accomplished under the rubric of "routine support" in target countries "well in advance" of hostilities. Of course, when the situation is not well in advance of hostilities, but there is operational planning for anticipated hostilities, then even the examples of "other-than-routine" support could occur as traditional military activities, as long as they are carried out under the direction and control of a military commander.

The next part of the article is a non-comprehensive historical survey of certain types of military activities compared in parallel with hypothetical military activities in cyberspace. It is not an attempt to comprehensively define what is meant by "routine support" or even "traditional military activity." Instead, each historical section is intended to provide factual, historical context for the subsequent section that follows discussing hypothetical military activities in cyberspace. The activities covered in the next section are suggestive of the outcomes that military use of information-based actions could achieve in anticipation of, or during, hostilities. The analogous information-based activities, when undertaken under the direction and control of a military commander, would be traditional military activities and not covert action.

[53] Compare with the exception for collection of intelligence.

II. Achieving Surprise

In the late 1970s and early 1980s, a number of significant studies were published in the military strategy field on the subject of surprise attacks.[54] Strategic thought in the 1960s tended to discount the utility of surprise in warfare due to the explosion in the number and type of technical means of intelligence collection. Extensive collection capabilities, it was thought, would provide the amount of indications and warnings of surprise attack that were missed at Pearl Harbor and on multiple occasions during the Second World War. The impetus behind this wave of scholarship on the utility of "strategic surprise"[55] in warfare was the success of both sides in the Arab-Israeli Wars in achieving surprise at various times.[56] Significantly, in both the Six Days' War (1967) and the Yom Kippur War (1973), surprise was achieved at the initiation of hostilities.[57] The two most detailed studies, Richard K. Betts's *Surprise Attack* and *Strategic Military Surprise*, edited by Klaus Knorr and Patrick Morgan, both reach the same conclusion: regardless of improvements in technology, intelligence and decision-making processes, strategic surprise in war will continue to successfully occur.[58] Twenty years later, the al Qaeda attacks on September 11, 2001, demonstrated the truth and staying power of that conclusion.

---

[54] See, e.g., STRATEGIC MILITARY SURPRISE (Klaus Knorr & Patrick Morgan, eds. 1982); BETTS, supra note 47.

[55] Klaus Knorr and Patrick Morgan define "strategic surprise" based on purpose and context, where the purpose is "to inflict a striking defeat that sharply alters the military situation and possible determines the outcome of the conflict." Klaus Knorr & Patrick Morgan, *Strategic Surprise: An Introduction*, *in* STRATEGIC MILITARY SURPRISE 1 (Klaus Knorr & Patrick Morgan, eds. 1982). In contrast, Richard K. Betts, a contributor to the Knorr-Morgan volume, in his later book provides a much broader definition, stating that "strategic surprise occurs to the degree that the victim does not appreciate whether, when, where, or how the adversary will strike." BETTS, supra note 47, at 4.

[56] The outcome of the Yom Kippur War in 1973 also led to a number of Israel-authored studies focused on that conflict, such as MICHAEL I. HANDEL, PERCEPTION, DECEPTION AND SURPRISE: THE CASE OF THE YOM KIPPUR WAR (1976) and a later, more comprehensive treatment. *See* URI BAR-JOSEPH, THE WATCHMAN FELL ASLEEP: THE SURPRISE OF YOM KIPPUR AND ITS SOURCES (2005).

[57] Unlike Knorr/Morgan and Betts, Ephraim Kam takes the narrow view that "the outbreak of war by surprise attack as a specific—indeed the most complex—instance of strategic surprise." EPHRAIM KAM, SURPRISE ATTACK: THE VICTIM'S PERSPECTIVE 2 (Harvard University Press 2004).

[58] BETTS, *supra* note 47, at 8 ("there is reason to doubt that precedent can steer defense planning away from the pitfall of surprise"); Klaus Knorr, *Lessons For Statecraft*, in STRATEGIC MILITARY SURPRISE 264 (Klaus Knorr & Patrick Morgan, eds. 1982) ("It is our overall conclusion that the business of minimizing strategic surprise faces

There are distinct parallels between these studies of strategic surprise and modern-day information operations. First, the language is often similar. For instance, "strategic surprise" theorists often speak of increasing the "noise" in order to increase ambiguity or deceive decision-makers. Information operations theorists also speak of "noise" either generated by information operations or information operations used defensively to reduce "noise." "Perception" comes into play in both efforts at strategic surprise and information operations. Another parallel, so close as to constitute an intersection, in fact, is the use of deception. As will be shown, deception operations are critical to achieving strategic surprise. And, at least in U.S. doctrine, deception and psychological operations are important components of information operations.

These similarities and parallels point to strategic surprise as a valuable lens through which to understand how some of the more intrusive, and potentially controversial, information-based actions possibly available to the United States should be viewed as traditional military activities. The following sections of the article examine two of the many factors that are identified with successful strategic surprise: getting forces into attack position, sometimes, but not always, secretly and deception operations. The article will proceed in parallel, with each section on a strategic surprise factor immediately followed by a section examining possible uses of information-based actions to accomplish the same or similar outcomes. In this way, it will be seen that this modern modality of warfare--involving networks, computers and information systems--can be used for purposes with roots buried deep in military strategy and traditions.

A. Positioning of forces: Historical Overview

---

odds that... are very formidable indeed."); HANDEL, *supra* note 56, at 7 ("[The five paradoxes described] tend to strengthen my pessimistic conclusion that there is little chance…to prevent or forestall an impending surprise attack. Very few surprise attacks on the strategic level have ever failed."); KAM, *supra* note 57, at xxv (stating that the first edition of the book "presents a rather pessimistic conclusion, namely, that it is at best very difficult to prevent surprise attacks" and stating that "the lessons of the last fifteen years support this conclusion").

There are many ways forces get in position for surprise attacks. Fortune is often involved; secrecy rarely. All too often, the attacking forces are seen or observed, but the importance of the observation is either discounted or misinterpreted. An example of the latter occurred at the Battle of Quebec (September 13, 1759) during the French and Indian Wars. The French forces in Quebec thought that the St. Lawrence River was unpassable for British shipping upstream of the city. The British discovered that it was not. On their way up past the city, the British ships were spotted by French sentries who thought the ships were a scheduled supply convoy from Montreal, downriver from Quebec. Fortuitously for the British, the sentries were not told of the convoy's cancellation, so they did not raise the alarm. The British managed to get upriver, land their forces on the Plains of Abraham and defeat the French.[59]

Luck, of course, plays a role in any military operation, but planning and preparation go a long way toward making one's own luck. In 1941, Japanese carrier forces approached Hawaii from the Northwest. The direction was unexpected not only because it was outside the usual shipping lanes, but also because it was generally thought that weather in that region of the Pacific, at that time of year, would prevent such an approach.[60] The Japanese managed to scout the route, though, using a three-man team of Naval officers on a Japanese commercial vessel that traveled the northern route from Japan to Hawaii.[61] The officers did not see another vessel on the entire trip and they were able to determine the outer boundary of U.S. aerial surveillance from Hawaii, critical facts to the success of the surprise attack against the U.S. Fleet in Pearl Harbor.[62] The Japanese Fleet was never observed by another vessel during its approach to the

[59] The facts in this paragraph are drawn from PAUL K. DAVIS, 100 DECISIVE BATTLES FROM ANCIENT TIMES TO THE PRESENT: THE WORLD'S MAJOR BATTLES AND HOW THEY SHAPED HISTORY 246-47 (1999).
[60] GORDON PRANGE, AT DAWN WE SLEPT: THE UNTOLD STORY OF PEARL HARBOR 227, 232 (Penguin Books 1991). In addition, the main Japanese thrust was believed to be planned against the Phillipines.
[61] *Id.*at 315-16.
[62] *Id*. at 316.

launch point. That secrecy was maintained through strict radio silence during the course of the voyage from Japan.[63]

In a similar fashion, strict radio silence was observed in the approach of nearly the entire Israeli Air Force against Egyptian airfields at the start of the Six Days' War in 1967. The silence was so strenuous that "[e]ven a pilot who had to bail out on the way to the target could not report his position."[64] Unlike the Japanese at Pearl Harbor, the Israeli's specifically chose not to attack at dawn. Instead, they waited until 8:45 AM, after Egypt's early morning patrols had returned to base and the Egyptians, who expected any attack would come at dawn, assumed the day would be a routine one.[65] Apparently, the time was not pushed later because the Israelis knew that senior Egyptian Air Force leaders would be on their way, but not yet at work at the time of the strike.[66]

In many cases, the forces are built up gradually, as the Germans did in the Ardennes before the Blitzkrieg into France in 1940. Allied forces were surprised not only by the location of the breakthrough, but also the speed and strength of the assault.[67] The gradual German buildup was aided by the fact that the French and British were focused on German forces accumulating on the Low Country borders, in a manner reminiscent of the start of the First World War.[68] Although Knorr terms this a "deception,"[69] it was actually more of a distraction, as the German force actually did invade and march through the Low Countries of Belgium and Luxembourg enroute to France.

---

[63] *Id*. at 741-42.
[64] Michael Handel, *Crisis and Surprise in Three Arab-Israeli Wars*, *in* STRATEGIC MILITARY SURPRISE 134 (Klaus Knorr & Patrick Morgan, eds. 1982).
[65] Coming from the direction of Israel, attack aircraft would have the rising sun behind them and make it much more difficult for defenders to see and target the attacking aircraft. *Id*. at 133.
[66] *Id*.
[67] *See* Klaus Knorr, *Strategic Surprise in Four European Wars*, in STRATEGIC MILITARY SURPRISE 26 (Klaus Knorr & Patrick Morgan, eds. 1982).
[68] *Id*.
[69] *Id*.

Many surprise attacks occur with the attacking forces in plain sight. This happened in the Second World War when Germany invaded Russia, the Yom Kippur War of 1973, the ground aspect of the Six Days' War, and Chinese intervention in the Korean War. The presence of these forces was often explained through intentional deception operations or misperceptions by the defending party, and sometimes both. These aspects will be explored in succeeding sections.

B. Positioning in Cyberspace: Access and Action

There are two aspects to "force positioning" in information-based actions against networks, computers or other information systems. The first aspect is about gaining access to the targeted network, computer or system. To conduct information-based actions, it is usually necessary to exploit a vulnerability in the system in order to get inside the system. Once inside, one of the activities that can then be carried out is information-based actions that enable the "force positioning" of conventional forces. This latter point is the second aspect of "force positioning" related to information-based actions.

A recent National Research Council study describes two types of access for conducting information-based actions: remote access and close access.[70] Remote access uses techniques to access a network, computer or information system from a distance, often, but not always, using the internet as the delivery vehicle.[71] Examples include the use of malicious software, such as viruses or worms; router attacks; use of botnets; protocol compromises; and security compromises.[72] Close access techniques are used to access computers or systems that are not able to be accessed remotely, generally because they are either not connected to other networks

[70] TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 87 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin, eds., 2009) [hereinafter TECHNOLOGY, POLICY, LAW].
[71] *Id*.
[72] *See generally id*. at 92-100 (discussing each of these approaches to remote access in detail).

("air gapped") or because they are stand-alone systems, such as weapons systems.[73] Access to such systems often requires either physical proximity to the targeted computer or system or access to some level of the supply chain for the targeted equipment or system.[74]

Whether access is achieved in a remote or close fashion, the objective of access, at least in the context of warfare, is to provide the ability to carry out a future action. As Martin Libicki points out, "it is easier to set up [such] conditions in peacetime. . . before the target's security posture is tightened."[75] Access then allows for either the concurrent or later introduction of a payload designed to carry out specific actions against the network or information system. Possible actions include altering data, destroying data, sending false messages, or causing systems to malfunction or stop working. So, in this context, "force positioning" in information operations will often involve peacetime access, either through remote or close means, in preparation for later actions during hostilities.

Most readers will be familiar with many of the examples of remote access delivery of payloads from media coverage of destructive worms and viruses set loose indiscriminately by hackers. Less familiar may be examples of close access to systems for the purpose of carrying out information-based actions. What I have elsewhere referred to as "chip-level actions"[76] is a prime example. Due to the multiplicity of methods for compromising micro-chips and the difficulty of detecting those problems, the micro-chip supply chain presents significant opportunities to introduce vulnerabilities into systems. As an example, in 1982 the CIA

[73] *Id*. at 87.
[74] See *id*. at 101-3 (discussing close access approaches in detail).
[75] MARTIN LIBICKI, CYBERDETERRENCE AND CYBERWAR 148 (2009).
[76] *See* Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 4 J. NAT'L SECURITY L. & POLICY, at 36 (forthcoming 2010).

managed to place "[c]ontrived computer chips. . . into Soviet military equipment,"[77] as part of a covert operation that involved a Canadian company in the Soviet supply chain.[78] It has also been reported that the French place compromised chips into the export versions of their missiles, so that they can be disabled if they are ever used against French forces, either by the purchaser or if they fall into the hands of others.[79]

This type of payload is known as a "kill switch," although the functionality implicit in that term is not limited to simply disabling a system. To the extent the term embodies the idea of disabling the functionality of a particular system, Libicki terms that type of action "disruption," defined as "render[ing] military systems temporarily incapable to a greater or lesser degree, leaving a different window of opportunity to be exploited vigorously."[80] Among the "legion" examples he provides are "command-and-control systems that suddenly refuse to function, sensors that go black, weapons whose electronics hang up (which prevents modern weapons from functioning, even in a debased or manual mode)." [81] Payloads that cause disruption are essential to the second aspect of "force positioning" in information-based actions. Disruptions to particular systems can be used to enable the positioning of conventional forces to carry out attacks, either undetected or with little opposition or warning.

Both Libicki and the National Research Council study point to air defense systems, often called integrated air defense systems (IADS), as an example.[82] The NRC study calls this a "force-multiplier effect" because such an action "could disrupt the network's operation in

---

[77] *See* Gus W. Weiss, *The Farewell Dossier: Duping the Soviets*, 39 STUDIES IN INTELLIGENCE (1996), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm;;
[78] *See* THOMAS C. REED, AT THE ABYSS: AN INSIDER'S HISTORY OF THE COLD WAR 266-70 (2004).
[79] *See* Sally Adee, *The Hunt for the Kill Switch*, IEEE SPECTRUM, http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0, at 1.
[80] LIBICKI, *supra* note 75, at 146.
[81] *Id*.
[82] *Id*. at 156; TECHNOLOGY, POLICY, LAW, *supra* note 70, at 91.

concert with a hostile flight operation, potentially blinding the defense system for a period of time."[83] There are claims that this is precisely what happened when the Israeli Air Force bombed a suspected Syrian nuclear facility in September, 2007. According to reports in the technical press, "higher-level, nontactical penetrations. . . of the Syrian command-and-control capability" led to the failure of the Syrian system to respond to the incoming Israeli jets.[84] Speculation centered on the possibility that "the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden 'backdoor' inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips' function and temporarily blocked the radar."[85]

In these kinds of systems, the compromised chip (or software, for that matter) doesn't have to actually "kill" the system. Instead, the system can be disrupted or degraded in a number of different ways to permit the kinetic attack to proceed undetected or unmolested: "by not seeing the target, seeing too many targets, failing to give or receive cuing information, not getting missiles to fire, firing missiles in directions that do not let them hit the target, or inappropriately emitting detectable energy."[86] Libicki goes on to point out it is the military, not intelligence operatives, that are best situated to understand which of these many options would be most effective.[87] According to Libicki, not only do military operators have the best understanding of how such systems work, but they will better comprehend the actions that the adversary military will take when such systems fail.[88]

---

[83] *Id*.
[84] *See* David A. Fulghum, Robert Wall & Amy Butler, *Cyber-Combat's First Shot*, AVIATION WK. & SPACE TECH. 26 Nov. 2007 (citing U.S. intelligence analysts for the assessment that this occurred as the result of "network attack" and providing a timeline of the assault on the suspected reactor).
[85] Adee, *supra* note 43, at 1.
[86] LIBICKI, *supra* note 75, at 156.
[87] *Id*.
[88] *Id*. ("Those most likely to understand such failure modes –and thus those best placed to plan a military campaign that uses operational cyberwar—are likely to be those who understand how their own systems might fail.").

"Force positioning," then, in information-based operations means not only the access necessary to carry out "cyberattacks," such as the action to take down the insurgent website that has been referred to throughout this paper. Positioning "force" in these kinds of operations also means preparations to carry out information-based actions that support kinetic attacks. Often, neither the action to gain access nor the disruptive action will themselves be actual "attacks," as defined in international humanitarian law. Instead, as can be seen by the parallel with the analysis of surprise, such actions are precisely the types of support to military operations that the military has traditionally conducted. Regardless of how close they occur to anticipated hostilities, the types of actions[89] described in this section should be treated as "traditional military activity" when they occur under the direction and control of a military commander.

Less clear, though, is whether such actions can be viewed as "routine support" to military operations when the timeframe is "well in advance" of any hostilities. Part of the difficulty, as previously discussed, is the ambiguity of the phrase "well in advance." In addition, using the supply chain to gain close access to a system will often involve the use of third-parties that may or may not be foreign nationals of the targeted state. In fact, of course, the activities described in this section are not "routine" in any sense of the word. Instead, these activities are directly related to the conduct of hostilities, either current or anticipated. The fact that access to targeted systems is required and obtained for purposes of executing military attacks is a clear indication that these are traditional military activities, not routine support, and should be regarded as such regardless of when they occur.

[89] This specifically includes supply chain actions to obtain close access to adversary weapons systems in order to prepare for their degradation and disruption on the battlefield, during hostilities. It is true that the example provided in the text was done by the CIA, possibly as a covert action though that is not clear from the sources, but it was also done prior to enactment of the current statutory definition of covert action. The contention in this paper is that the military could execute such an operation as a "traditional military activity" during ongoing or anticipated hostilities.

C. Deception Operations: Historical Overview

Deception has a long history in warfare. Although probably apocryphal, the story of the Trojan Horse in ancient Greece is one of the world's most well-known deception operations: Odysseus and his thirty Greek warriors hiding inside, waiting for the Trojans to pass out after their feast, then open the gates for the Agamemnon's Greek army to invade and sack Troy.[90]

There are many, many instances of the use of deception to achieve tactical surprise in specific battles. For instance, George Washington used disinformation to disengage from British forces around New York City in order to march to Virginia, join forces with Rochambeau and defeat Cornwallis at Yorktown.[91] In the Second World War, deception operations were routinely implemented before battles.

Most famous of all was the creation of a dummy army (literally) under General George Patton prior to the invasion of Normandy.[92] In the deception operation, Patton's phony army was deliberately placed in England across the Channel from Pas de Calais.[93] This served to reinforce German, particularly Hitler's, belief that the invasion of France would come at Calais.[94] Patton's "army" maintained the level of radio traffic and communications that would be expected of a force that size.[95] In the other famous World War II tactical deception operation, "Major William Martin," *The Man Who Never Was*,[96] washed up on a Spanish beach with a briefcase of sealed documents that were surreptitiously examined by the Germans.[97] The information learned

[90] *See* Robert Graves, *The Wooden Horse*, in FROM TROY TO ENTEBBE 4-5 (John Arquilla, ed. 1996).
[91] PAUL K. DAVIS, 100 DECISIVE BATTLES FROM ANCIENT TIMES TO THE PRESENT: THE WORLD'S MAJOR BATTLES AND HOW THEY SHAPED HISTORY 260 (1999).
[92] *See* NICHOLAS RANKIN, A GENIUS FOR DECEPTION: HOW CUNNING HELPED THE BRITISH WIN TWO WORLD WARS 398-399 (2009).
[93] *Id*. at 398.
[94] *Id.* at 399.
[95] *Id*.
[96] EWEN MONTAGU, THE MAN WHO NEVER WAS (1953).
[97] *Id*. at 123. This idea was actually a much grander version of the deception plan carried out by the British before the Third Battle of Gaza in the First World War. *See* MICHAEL I. HANDEL, WAR, STRATEGY AND INTELLIGENCE 368

caused Hitler to move forces from Sicily to Sardinia and Greece.[98] The Allies successfully landed on Sicily, facing minimal opposition[99] as Hitler continued to believe that Sicily was a diversion and the main blow would fall on Greece.[100] Although the focus of this section is on use of deception to accomplish strategic surprise, these Second World War examples are noteworthy because the results of each were monitored nearly contemporaneously. This was accomplished thanks to intelligence from the Ultra program, a British program that intercepted and decoded German messages due to their analysis of a captured German Enigma code-machine.[101]

Elaborate deception operations often precede the initiation of hostilities between states. Many times, the deception operation is used to explain the proximity of the attacker's troops to the target of the attack. In the Second World War, for instance, Richard Betts's study found that "[d]eception and disinformation campaigns were integral to planning and coordinating all Hitler's surprise attacks."[102] As an example, prior to Operation Barbarossa, the German invasion of the Soviet Union, the Soviets were aware of the massive buildup of German divisions near Soviet borders. Germany, however, led the Soviets to believe that the buildup was for "Operation Sea Lion," the plan for the invasion of Great Britain. As part of the deception plan, Germany increased its propaganda towards Great Britain and stopped it against the Soviet Union,

---

(1989). In that deception operation, a British haversack was "lost" in such a way that it was recovered by the German-Turkish forces defending Gaza. *Id*. The haversack's contents indicated that the main British attack would come at Gaza, which reinforced existing German-Turkish perceptions, *id*. at 370, and that the attack on Beersheba would be a diversion. The haversack also contained various accoutrement--what today is called "pocket litter"--such as a personal diary, a small amount of cash, and "private" letters of soldiers supposedly stationed near Beersheba complaining about the idea of attacking Gaza. *Id*. at 368. As with the later invasion of Sicily, even after receiving reports about the size of the British force attacking Beersheba, the German-Turk High Command continued to believe that was a feint and that the real attack would come at Gaza. *Id*.

[98] MONTAGU, *supra* note 96, at 6.

[99] *Id*. at 126.

[100] *Id*. at 143.

[101] STEPHEN E. AMBROSE & RICHARD H. IMMERMAN, IKE'S SPIES: EISENHOWER AND THE ESPIONAGE ESTABLISHMENT 62-4, 84 (1981).

[102] BETTS, *supra* note 47, at 40. Betts's book is also the source for the rest of this paragraph.

creating a "calm before the storm effect." At the same time, Germany executed heavy air raids against Great Britain while publicly redeploying some divisions westward. German commanders in the area of the buildup were also ordered to build field fortifications that could serve no offensive purpose. This suggested to the Soviets that the secondary purpose of the buildup was designed to defend against a possible Soviet attack. The German deception fed into and reinforced Stalin's self-deception about the German buildup.

Deception played a significant role in each of the Arab-Israeli Wars.[103] Prior to the 1973 Yom Kippur War, for instance, the Egyptians and Syrians used "elaborate deception" to achieve surprise.[104] They consciously attempted to maintain a facade of routine activity, including the use of "exercises" as a cover for troop movements.[105] Taking a page from the Israeli playbook in 1967,[106] the Egyptians demobilized 20,000 troops 48 hours before the attack.[107] In addition, the Egyptians and Syrians had intentionally spread rumors over an extended period of time regarding alleged shortages of spare parts for their Soviet military equipment.[108] This contributed to American and Israeli intelligence assessments about the weakness of the Arab forces. Those assessments, in turn, contributed significantly to the perceptions of Israeli decision-makers that it would be foolhardy for the Arab forces to attack the militarily stronger Israel.[109]

---

[103] In 1956, Israeli actions were intended to give the impression that Jordan, not Egypt, would be the target of any attack. *See* HANDEL, *supra* note 97, at 319. Prior to the Six Days' War, Moshe Dayan, newly installed as Defense Minister, gave a prominent interview asserting that "(1) it was too late to react unilaterally to the blockade of the straits, (2) Israel had the capacity to maintain mobilization for a long time, (3) Israel could fight successfully after absorbing the first blow, and (4) it was too early yet to know whether diplomatic action would prove futile." BETTS, *supra* note 47, at 66. Other steps, such as giving thousands of troops leave and ensuring that photographs of soldiers relaxing on the beach, contributed to this deliberate "aura of unconcern." *Id*. Israel attacked 38 hours after Dayan's interview. *Id*.

[104] Michael Handel, *Crisis and Surprise in Three Arab-Israeli Wars*, *in* STRATEGIC MILITARY SURPRISE 137 (Klaus Knorr & Patrick Morgan, eds. 1982).

[105] *Id*.

[106] See *supra* note 103.

[107] Handel, *supra* note 97, at 137.

[108] *Id*.

[109] *See id*. at 139 ("The Israelis therefore incorrectly assumed that the Egyptians and Syrians would not open a war in which they would lose, particularly because of the 1967 debacle"); see also Betts, supra note __, at 69 (stating that

More recently, deception played a role in the 1991 Gulf War. Although the initiation of hostilities was probably not a surprise to Saddam Hussein given the United Nations Resolutions and President George H.W. Bush's deadline, the location of the coalition's main attack was considerably uncertain to Hussein and his Generals. Contributing to this uncertainty was General Schwartzkopf's use of Marine Amphibious Forces as a decoy to convince Hussein that at least a significant portion of the assault would be an amphibious landing from the Arabian Gulf.[110] Preparations even went so far as to include Navy SEAL teams conducting pre-landing reconnaissance and beach marking activities.[111] They also placed explosive charges on the beaches that were later blown up as the SEALs went back forth along the Iraqi defenses firing tracers to simulate the initial phase of an amphibious landing.[112] As a result, Hussein shifted two divisions of troops away from the Saudi border area, weakening the area of the main coalition assault.[113]

D. Deception Operations in Cyberspace

"Cyberattacks are about deception, and the essence of deception is the difference between what you expect and what you get: surprise. This is why operational cyberwar is tailor-made for surprise attack."[114] Here, deception works on two levels. Information-based actions are deceptive by nature because of the inherent difficulty in attribution. For purposes of this paper, that means that such actions are usually not apparent or acknowledged at the time they occur. As we have seen, in the appropriate contexts the lack of acknowledgement will not usually matter for traditional military activities. The second level of operation is the use of information-based

---

observed Arab preparations did not lead to warning of imminent attack because of "the overpowering political and military preconceptions of Israeli (and American) officials. Strategic premises smothered tactical indicators.").
[110] ROBIN NEILLAND, IN THE COMBAT ZONE: SPECIAL FORCES SINCE 1945 296-97 (1998).
[111] *Id*. at 297.
[112] *Id*.
[113] *Id*.
[114] LIBICKI, *supra* note 75, at 143.

actions for deception operations in support of conventional, or kinetic, military operations.[115] Given the statement that information-based actions are "tailor-made" for supporting surprise attacks through deception, it is somewhat disconcerting to find very little discussion in the unclassified information operations literature about surprise attacks, or even deception. Deception, usually called "military deception," is one of the pillars or core functions of Information Operations.[116] Yet, it usually gets short shrift in Information Operations treatments, despite the fact that its use to achieve surprise is a well-recognized force multiplier and the costs of deception operations to the benefits achieved are low.[117]

Deception is all about information: controlling what is known about your actions and operations by either hiding them or feeding false information to your adversary. The best way to feed a networked adversary false information, or even true information that may not be the entire truth, is to have access to the adversaries information system. Once inside the system, it might then be possible to send bogus email traffic that "could easily provide misinformation regarding the military capabilities, intentions, locations, and operations of friendly forces."[118] Such emails could allow friendly forces to move into favorable attack positions ala the British forces at

---

[115] *Id*. at 139. Libicki defines "operational cyberwar" as "the use of a computer network attack to support physical military operations," which should be compared with his concept of "strategic cyberwar" where the primary mode of warfare is state-to-state "campaign[s] of cyberattacks" with no, or very little, active hostilities taking place. Id. at 117. Libicki doubts that strategic cyberwar, by itself, can provide sufficient coercion at the State level, primarily because sufficient, sustained suffering cannot result from cyberattacks that are easily mitigated, hard to maintain, much less duplicate, *id*. and "cannot occupy territory; put people's lives at risk; or, except in specialized cases, break things." *Id*. at 140.

[116] Dan Kuehl, *Introduction: "Brother, Can You Spare Me a DIME?"*, *in* INFORMATION WARFARE: SEPARATING HYPE FROM REALITY (Leigh Armistead ed., 2007) (listing military deception as a "core competency" of Information Operations).

[117] Barton Whaley, *The One Percent Solution: Costs and Benefits of Military Deception*, *in* INFORMATION STRATEGY AND WARFARE: A GUIDE TO THEORY AND PRACTICE 127 (John Arquilla & Douglas A. Borer eds., 2007).

[118] TECHNOLOGY, POLICY, LAW, *supra* note 70, at 178. Some of this could also be accomplished by what Libicki calls "corruption," examples of which are "a sensor that fails to pick up on certain types of signals, seems less sensitive that (sic) it should be, or misinterprets what it sees; a communication system that misroutes packets or leaves some nodes mysteriously in the dark." LIBICKI, *supra* note 75, at 147.

Quebec.[119] Return emails to the adversary "originator" "could be intercepted and appropriately modified before being displayed to the ["originator"]."[120] Access inside a command and control network would allow the "spoofing or impersonation of legitimate authorities" to send false information or disrupt the link between the forces in the field and the adversary state's leadership.[121]

Of course, access at a sufficiently high level of the network or system may permit the injection of information directly into the adversary's decision-making process rather than through indirect sources,[122] such as the media or through deceptive operational policies and practices. For the analysis presented in this paper, the purpose of such an action, as well as the target, will be important for the covert action-traditional military activity issue. If the purpose is to influence the political leadership of the adversary state, even if it is to deceive them as to time, place, etc. of an attack, that would easily fit within the covert action definition. A strong argument could be made under the legislative history that if hostilities were imminent, such activity could be a traditional military activity if it were under the direction and control of a military commander. As a policy matter, such an argument would be better used on the shelf rather than on the table. Political influence operations, probably even in a time of hostilities, are best left to the CIA and/or the national command authority. After all, given the scope of some of the deception operations discussed in Part II.C (the interview provided by Minister of Defense Moshe Dayan before the Six Days' War; Hitler's involvement with deception for Operation Barbarossa), it is apparent that such high-level efforts are essentially not under the direction and

[119] *See infra* note 59 and accompanying text.
[120] TECHNOLOGY, POLICY, LAW, *supra* note 70, at 178.
[121] *Id*. at 179.
[122] MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE 119 (2007). Libicki also points to the importance of knowledge about the adversary leadership in order to effectively tailor information-based influence messages, much as the deceptions surrounding Operation Husky (Allied invasion of Sicily) and Operation Barbarossa (German surprise attack on Russia), played into the preconceptions of Hitler and Stalin, respectively. *Id*.

control of a military commander. Instead, the closer the information-based deception operation gets to the actual battlefield and targets adversary military commanders in specific instances, then it is truly the "traditional military activity"[123] contemplated by Congress. For example, information-based deception operations analogous in scope and immediacy to the decoy amphibious landings in advance of Desert Storm in 1991 would be a traditional military activity.

Between these two extremes (strategic-political deception and short duration tactical deception) is the theater-level deception operations prior to the invasions of Normandy and Sicily. The target of each was clearly not just the local commander on the ground, but also the political leadership in the form of Hitler. Although the decoy/deception operation in advance of Desert Storm also included Saddam Hussein in its scope, the preparation and duration of the deceptive activity was much less and shorter in duration than that for Normandy and Sicily. The significant commonality between Normandy, Sicily and Desert Storm was they were all under the direction and control of a military commander. Elements on the staff of each military commander were responsible for the planning and execution of each operation, which themselves were conducted in large measure by military personnel. This places such theater-level information-based deception actions and operations decidedly on the ground of traditional military activities or "routine support" for military activities when preparations for such actions/operations occur "well in advance" of hostilities.

III. Conclusion

The first step to ensure the military can respond as rapidly as possible to networked adversaries, whether terrorists or states, is to make clear that military commanders in the Department of Defense do not have to make reports to Congress before taking appropriate and

[123] Or "routine support" for military operations, if the preparations for such tactically-oriented deception operations occur "well in advance" of hostilities.

necessary measures in carrying out their duties. Despite any misconceptions to the contrary in the popular press, Congress made its intent very clear by making the military commander the fairly bright line test for what is "traditional military activity." Part I demonstrated that Congress placed no substantive limit on this definition during ongoing hostilities or prior to anticipated hostilities. This is the case whether the activity occurs on the ground, in the air, or in cyberspace (networks, computers and information systems).

As the historical parallels to information-based actions and activities show, there is a wide range of such actions that are traditional military activities not only because they are under the direction and control of a military commander, but also because they are conducted for purposes directly tied to or in support of military operations. Access to networks, computers and information systems is endemic to the range of computer network operations, including exploitation, attack and defense. At the strategic level, when an information-based deception operation passes into the political realm and out of the direction and control of a military commander, it is no longer a "traditional military activity," though more tactical, scaled-down efforts at the theater and battlefield level remain traditional military activities when controlled by military commanders.

Finally, it is appropriate to return to the beginning and consider anew the questions raised by the shutdown of the extremist website by the U.S. military. The questions it posed[124] are easily addressed based on even a cursory review of the legislative history: during ongoing hostilities,

[124] The two questions posed that this article addresses are: "Is taking out an extremist Web site a covert operation or a traditional military activity? Should Congress be informed?" Nakashima, *supra* note 1, at A1. The third question, "When is a cyberattack outside the theater of war allowed?", is beyond the scope of this article, but suffice to say that there is not enough information in the article to determine the basis for the factual assumption underlying the question, i.e., that it occurred "outside the theater of war."

the action by a military commander to eliminate a recruiting and operational planning tool of the adversary is a traditional military activity that does not have to be reported to Congress. Given the ease with which this conclusion is reached, one has to conclude that the "complex [legal] questions" are merely a red herring thrown out by those who lost a policy debate. The significant point to draw from the article is that there was, in fact, a debate that occurred within a formal process. And, importantly, that process included not just Defense and military officials, but also CIA officials.

This kind of extensive, interagency policy debate was precisely what did *not* occur during the Iran-Contra affair that led Congress to pass covert action reporting statute in 1991. Improved processes of review, in fact, are exactly what Congress did in the Intelligence Authorization Act for 1991, building on previous attempts to instill process through the Hughes-Ryan Amendment and the Intelligence Oversight Act of 1980. In fact, even in the covert action process today, the Defense Department does not have a formal role in reviewing proposed covert actions, which is largely a CIA-National Security Council process, with the Director of National Intelligence playing a secondary role. Congresses concern about lack of process for covert action was not present in the Defense Department. Rigorous and detailed Defense processes, such as occurred in the case of the extremist web site and the very formal, long-standing Defense Department war planning process, justified Congress providing a broad exception for traditional military activities.