This article was downloaded by: [United States Military Academy]
On: 15 January 2015, At: 08:07
Publisher: Routledge
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK

International Journal of Intelligence and CounterIntelligence
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ujic20

Cyber Actions by State Actors: Motivation and Utility

Aaron F. Brantly

Published online: 12 May 2014.

CrossMark
Click for updates

To cite this article: Aaron F. Brantly (2014) Cyber Actions by State Actors: Motivation and Utility, International Journal of Intelligence and CounterIntelligence, 27:3, 465-484, DOI: 10.1080/08850607.2014.900291

To link to this article: http://dx.doi.org/10.1080/08850607.2014.900291

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms &

Conditions of access and use can be found at http://www.tandfonline.com/page/terms-and-conditions

Downloaded by [United States Military Academy] at 08:07 15 January 2015

International Journal of Intelligence and CounterIntelligence, 27: 465–484, 2014
Copyright © Taylor & Francis Group, LLC
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2014.900291

Downloaded by [United States Military Academy] at 08:07 15 January 2015

AARON F. BRANTLY

Cyber Actions by State Actors: Motivation and Utility

I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones.—Albert Einstein[1]

Covert action is as old as political man. The subversive manipulation of others is nothing new. It has been written about since Sun Tzu and Kautilya. People and nations have always sought the use of shadowy means to influence situations and events. Covert action is and has been a staple of the state system. A dark and nefarious tool often banished to philosophical and intellectual exile, covert action is in truth an oft-used method of achieving utility that is frequently overlooked by academics. Modern scholars contend that, for utility to be achieved, activities such as war and diplomacy must be conducted transparently. Examined here is the construction of utility for a subset of covert action: cyber attacks.

Cyber attacks, as a functional tool of state, have the ability to influence the space between overt diplomacy and overt war. They have been and are currently being used to influence what James D. Fearon refers to as the *ex-ante* bargaining range of states.[2] The manipulation of the bargaining range between states to achieve a more favorable *ex-ante* settlement that averts the potential for overt war is not limited to cyber attacks, however. Cyber attacks are just one tool among many that has risen in prominence in recent years.

Dr. Aaron F. Brantly is Adjunct Professor of Intelligence and National Security Affairs at the University of Texas, El Paso. A graduate of Queens University, Charlotte, North Carolina, he earned a Masters in Policy Planning from the American University, Washington, D.C., and his doctorate in International Relations from the University of Georgia. A specialist in Middle Eastern and Eastern European affairs, he served as a Peace Corps volunteer in Ukraine from 2005–2007.

Utility is a measurement of benefits accrued to a party engaging in a decision to do something. In this context, cyber attacks are a tool aimed at achieving positive utility for a state or entity attempting to employ them against an adversary to alter a bargaining range between two states prior to engaging in or in attempting to avert an overt war.

A DEVELOPING AREA FOR SCHOLARS

Cyber is an emerging field of study. As with any emerging field of study, definitions of terms often vary between scholars. The typologies of Computer Network Operations (CNO) are defined here in the context of the Joint Chiefs of Staff Joint Terminology Lexicon.[3] The three CNO typologies are: Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND). These definitions by their nature force the context of this discussion into an American-centric model for understanding the development of utility through actions undertaken in cyber. Table 1 provides the terms with their corresponding definition.

James Fearon noted that the central puzzle about wars is that they are costly, but still recur.[4] When creating a rational model for any form of conflict that model must of necessity be rooted in a motivation for conflict and, furthermore, the result of any conflict must have a measureable utility. States employ covert action against adversaries to narrow the bargaining range on issues to prevent, preempt, or minimize the extent of war. The motivation for using covert action is largely the same as that for all forms of conflict. Utility is thus defined as the ability to covertly alter an adversary's policy positions. Covert action, Track-II, or the "silent option," as it has often been known, allows for the bridging between the security dilemma of realism and the complex interdependencies of neo-liberalism.

Table 1. Typologies of Computer Network Operations[5]

CNE	Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
CAN	Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
CND	Actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks.

Downloaded by [United States Military Academy] at 08:07 15 January 2015

A useful rationalist argument for covert cyber attacks can be predicated on Fearon's "Rationalist Explanations for War."[6]

Setting the Basic Assumptions

Before diving into the motivation and rationality for conflict, establishing certain basic assumptions is necessary. First, rationality as a topic is reflective of bounded rationality which is used to more accurately reflect the conditions present within the international system, both within neo-realism and neo-liberalism. Herbert Simon has provided a guide to the context of bounded rationality as follows:

> To deduce the procedurally or boundedly rational choice in a situation, we must know the choosing organism's goals, the information and conceptualization it has of the situation, and its abilities to draw inferences from the information it possesses. We need know nothing about the objective situation in which the organism finds itself, except insofar as that situation influences the subjective representation.[7]

Second, at times a national leader might act out of self-interest rather than in the national interest. Covert cyber action conducted by a state may have positive utility for an individual leader of a state and may at the same time be irrational because it has a negative utility for the state. Such an instance would indicate that engaging in covert action would be irrational from a national security perspective. Leaders might act (and have) based on their individual rationality and still force their state to behave irrationally. Germany's Adolf Hitler would be a prime example of this. But, normally, states essentially act as unified rational actors in the national interest.

The Motivation and Rationality for Conflict

War is most commonly referred to as a violent kinetic act. Fearon stated that war, while often assumed to be *ex-ante* efficient, is virtually always *ex-post* inefficient.[8] He cited three commonly held rationalist arguments for why states are willing to engage in conflict despite knowing they are forgoing the lesser *ex-ante* costs of bargaining in favor higher *ex-post* costs associated with conflict. The most common assumptions for the causes of war as defined by Fearon are anarchy, preventative war, and positive expected utility. Each of these causal explanations for war has a substantial literature behind it.[9] Each in some way develops a logic for *casus belli*.

Kenneth Waltz, John Mearsheimer, and other neorealists argue that the security conundrum makes war inevitable because nothing within the international anarchic order prevents it. Fearon noted that while this is true, the lack of constraints on war occurring and the fact that wars occur

Downloaded by [United States Military Academy] at 08:07 15 January 2015

do not present sufficient grounds for rational conflict. He explained that despite a lack of constraints preventing war, the act of engaging in war is almost always *ex-post* inefficient and therefore irrational. Furthermore, he cited realist arguments that states engage in preventative wars as a rational act. Although realists argue that engaging in war at the present to minimize future costs is rational, Fearon showed that this is a flawed logic. *Ex-post* inefficiencies are still present in both anarchic and preventative war, which, according to Fearon, makes them both irrational.

In truth, the oft-cited rational reasons for war are not rational and are instead structural constraints that make war more likely. The ontological foundation and the epistemological limits of policymakers form the basis of structural constraints within the international system. These constraints then enable an *ex-ante* rational choice of war.

Where my assessment diverges somewhat from Fearon's notion of rationalist explanations for war is in his conceptualization of expected utility. Fearon indicates that a state with positive utility will often use this as an *ex-ante* basis for the instigation of what will become an *ex-post* inefficient war. But positive expected utility of one choice within a decision-set does not indicate that it will be the most rational choice within the decision-set. As war is typically only one option within a decision-set, the positive expected utility for the instigation of war against another state might prove to be of lesser value than other options. Positive expected utility simply indicates that a state having an outright negative utility for a particular option within a decision-set cannot rationally choose that option.

Intrapersonal Utility Options

Because the expected utility of international conflict is only one possible option in a range of policy options, its utility must be weighed against other options within the decision-set. Other options can include overt diplomacy, overt sanctions, or any number of policy paths. These policy options allow for an intrapersonal comparison of utilities, meaning that utilities are comparable across the decision-set within a single individual (or state). This differs from assumed utility construction in which decisions are identical across individuals (or states), or interpersonal utility construction. The subjective nature of utilities in a bounded sense of rationality makes interpersonal utility comparisons illogical.

Utilities of options within a decision-set facilitate preference ordering through intrapersonal comparison. Intrapersonal comparison indicates that if state A has a positive utility of .08 for conflict and a positive utility of .09 for covert cyber action, covert cyber action is likely to be ranked higher, based on a cardinal preference ordering of utilities. The utilities are not intrapersonally independent. This is an important distinction that

Downloaded by [United States Military Academy] at 08:07 15 January 2015

needs to be made in the rationalist explanations of war. While the first two explanations as posited by James Fearon are clearly predicated on weak rational explanations (because they are not causal explanations but structural frameworks), the third is not and more accurately underpins all aspects of rationality, as indicated by Herbert Simon.

Both Fearon and Bruce Bueno de Mesquita make the argument for the bounded rationality of actors. Within a bounded rationality model, the utility for conflict must be positive. Bueno de Mesquita does not explain why states go to war, only that the act of going to war with the conditions he presents is rational. The greater the utility, the more compelling the argument for war. He writes: "Being rational simply implies that the decision maker uses a maximizing strategy in calculating how best to achieve his goals."[10] This is a clear indication that rationality, in Bueno de Mesquita's conceptualization, is simply a way of ranking utilities to achieve the best result.

Claiming that rationality is predicated on a full understanding of the utility for conflict both *ex-ante* and *ex-post*, Fearon asserted that the motivation for conflict is largely based in three root causes. First, war can occur due to private information and incentives to misrepresent.[11] Second, war can occur due to commitment problems between states.[12] Third, war can occur due to issue indivisibilities.[13] In these situations negotiating an *ex-ante* settlement to avoid hostilities within Fearon's bargaining range of possible *ex-ante* solutions is not possible. For Fearon, the rational locus for *casus belli* lies in indivisibilities, misrepresentation and miscalculation, and commitment problems. Each of these roadblocks to an *ex-ante* bargain disproportionally affects the utility construction of the options within a decision-set and thereby facilitates a rationalist explanation for war.

RATIONAL BASES FOR WAR

Fearon's bargaining range points to three instances in which international conflict can be initiated rationally: (1) rational miscalculation due to a lack of information or a disagreement about relative power due to information asymmetries; (2) issue indivisibilities; and (3) commitment problems. But each of these rationalist explanations for war is predicated on the conflict initiator having a positive expected utility. Rarely if ever has there been a case in which two states have mutually and simultaneously declared to engage in hostilities against each other. Most if not all conflict has a conflict initiator. The definition of conflict initiator can at times be blurred, yet never have two states mutually agreed to settle their differences by engaging in warfare without one having fired the first shot.

Motivation and utility should be rightly separated when discussing war. While in realism the world is black and white, us and them, the complex

Downloaded by [United States Military Academy] at 08:07 15 January 2015

interdependencies of neo-liberalism offer a hybrid model for conceptualizing how states interact. Although Fearon claimed to be making an argument in support of realist rational explanations for war, he in fact made a neo-liberal argument. In essence he claimed that states are not confined purely to zero-sum interactions, but rather are defined by two competing measures of expected utility, the *ex-ante* and the *ex-post*. If anything, the bargaining range represents what Arthur Stein refers to as coordination and collaboration:[14] He writes:

> Regimes arise because actors forgo independent decision-making in order to deal with dilemmas of common interests and common aversions. They do so in their own self-interest, for in both cases, jointly accessible outcomes are preferable to those that are or might be reached independently.[15]

No mechanism is presented in the neo-realist literature by which states can achieve a bargaining stance *ex-ante*. Instead, the victor imposes its demands on the loser following the conclusion of hostilities, either as a requirement for concluding hostilities, or earlier as a requirement for avoiding hostilities. Both sides are thereby caught in a prisoner's dilemma and are willing to defect, creating an irrational (inefficient) *ex-post* result.

What Fearon attempted to illustrate is a situation in which states can create a mutually established agreement, a regime that seeks efficiency. His argument was in line with Bueno de Mesquita's view of the necessity for a positive expected utility. An alternative policy option to war that arises is necessarily compared to Bueno de Mesquita's concept of expected utility for international conflict. If the alternative course of action offers a higher utility, that option would be the rational choice. If options with greater political utility exist, these options should alter the expected benefits to be gained by conflict and alter the expected utility of conflict, creating a diminishing utility for conflict over time.

If a state has a negative utility for conflict, engaging in conflict would be irrational. Therefore, having multiple outcomes of the decision process is possible. A state can rationally engage in conflict, yet have other preferences that provide greater utility. Conflict could provide the greatest utility and therefore be chosen as the maximizing preference. Or, conflict could have a negative utility. In the final instance, choosing conflict would be irrational, regardless of the structural constraints of the system, thus seeking an alternative to conflict would be more logical. Every option has a measure of utility to the decisionmaker. Having utility does not equate to choosing a preference unless that preference provides a utility maximization.

In summary, conflict is rational in three instances where a mathematical means of assessing its rationality to engage in conflict is available. Yet, the

Downloaded by [United States Military Academy] at 08:07 15 January 2015

establishment of rationality behind conflict fails to sufficiently identify a motivation for conflict. Simply stating that issue indivisibilities are present is not a sufficient motivation for conflict; likewise information asymmetries and commitment problems do not provide a motivation for conflict. They instead describe the characteristics in which conflict can occur.

A policy range in which states interact defines their bargaining range. Figure 1 establishes the bilateral policy range between two states. Broadly stated, international relations are the process through which states influence one another's policies. The bilateral policy range is a relationship of policies between two states. The rational explanations for conflict can occur in this policy range. The focus here is on the bi-lateral policy range of states because, mathematically, covert action functions differently than overt operation with regard to the conceptualization of utility.

In Figure 1, at time T_n two states are aligned on a policy spectrum and the distance between them represents the difference between their respective policy positions. The more proximate the states are, the closer their policy positions. Likewise, the further they are apart, the more they diverge in their policy positions. Assuming state P_x is the potential conflict initiator, it looks for movement in the policy position of state P_x. State P_y has three options: it can (1) maintain the status quo, (2) move its policy further away from P_x, or (3) move its policies more in line with P_x. In this situation state P_x will likely view a policy shift away from its position as an act of aggression; it might also view the maintenance of the status quo as an act of aggression. Lastly, it might view the policy shift of state P_y as occurring too slowly, which could also be construed as a hostile action. Each instance presents a possibility for the potential conflict initiator to view the actions by its adversary as hostile. Option three is the least likely to be viewed as hostile, while option two is most likely to be viewed as hostile, with option one somewhere in between.

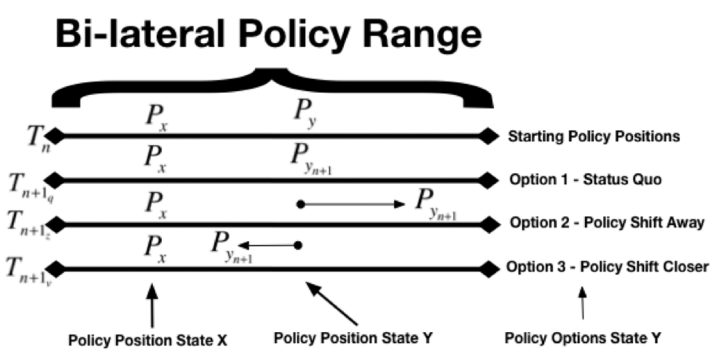

Figure 1. Bi-lateral policy range between states.

Downloaded by [United States Military Academy] at 08:07 15 January 2015

The motivation for any conflict is rooted in the policy divergences between nations on issues. Both neo-liberalism and James Fearon's claims for rationality indicate that in most instances a workable settlement can result in a more efficient outcome than war. Before resorting to war, and working within Fearon's identifiable areas preventing an *ex-ante* settlement, is another set of options open to policymakers that have been used for millennia in an effort to mitigate the rationalist explanations for war and provide a mechanism for facilitating an *ex-ante* settlement.

THE UTILITY OF COVERT ACTION

Covert action is a step into the breach short of overt armed conflict between two belligerents. It can occur throughout the policy interactions of states. Covert action serves as a tool for the mitigation of information asymmetries, issue indivisibilities, and commitment problems. It can serve as a tool to improve the bargaining position of a state or to bring states back to the bargaining table. Within covert action is a modern category of covert actions that are increasingly being used to influence the bargaining range: computer network operations.

But if covert action is truly a third option, its utility must be expressed in the context of the *ex-ante* and *ex-post* costs.

Utility and the Literature

Most often political scientists examine utility in the context of "Political Utility." Political is a complicated term likely to encompass predefined or conceived meanings. In this context, disaggregating the two terms comprising political utility is desirable. The first term, "politics," derived from the Greek term *politika* and examined in detail by such philosophers as Aristotle and Sun Tzu, is of little help in understanding the contemporary term political utility. Politics refers simply to the "art or science of government."[16] In contrast, "utility" is a powerful economic concept developed in exhaustive detail and honed into its modern form by Jon Von Neumann and Oscar Morgenstern.[17] The economic concept of utility was first carried over to political science in the 1950s with the work of Anthony Downs.[18]

Downs stated that utility is simply a "measure of benefits."[19] Following directly in the footsteps of Von Neumann and Morgenstern, he defined utility by explaining that a rational individual, given a series of alternatives, will weigh the values of each and create a *complete* and *transitive* order of preference, then choose the preference with the highest value. The economic terminology associated with utility is not related to the mutual understanding of preference orderings between two potential belligerents. Rather it is an individual decisionmaking process. Therefore, the utility

Downloaded by [United States Military Academy] at 08:07 15 January 2015

factor for two individuals in the same situation can differ dramatically. Conceptually, Downs explained this in writing that a voter will act towards "his own greatest benefit."[20] If all voters had the same utility calculus, elections would not be needed. To create political utility the terms are aggregated. For the purposes of understanding state action in international relations, and in the context of a unitary rational actor, political utility is the measurement of the benefits to government.

The concept of the benefits to government is not as straightforward as it might appear at first glance. In this instance, the government is assumed to be representative of the collective will or interest of the people. This might not be true in non-representative systems, yet, even within these systems, individuals must respond to their government; thus, to assume a diffusion of collective benefit or cost associated with a government's actions is possible by extension. These benefits and costs are not always distributed equally among the citizens of a nation. But, policy areas such as national defense are assumed to comprise common pool resources. Whether the motivation for an action originates internally or externally the utility scores are calculated based on what can be gained or lost in relation to the opponent. National gain or loss differs significantly from what might be gained or lost politically within a nation. An argument predicated on domestic political utility development functions separately from the one being posed here in relation to state-on-state covert action.

Political utility is not perfect and contains many failings. Many of these failings are found in the inability to aggregate individual preference orderings, the cognitive failings examined by Amos Tversky and Daniel Kahneman, or even in group dynamics as illustrated by Irving Janis.[21] Despite its limitations, no piece of literature finds that rational choices must be conditional upon an opposing party's simultaneous choice. Robert Grafstein has noted that "Conditional expected utility maximizers are concerned with expected utility, whether or not they caused it."[22] In most instances, rational decisions are reached independent of one another. Covert action has utility because it seeks to maximize the benefits to a government, and by extension to its people, in the same way as do overt diplomatic bargaining and overt military conflict.

The Use of Covert Action for Political Utility

The National Security Act of 1947 defined covert action as "[a]n activity or 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 acknowledged publicly."[23] In an international system where the formal declaration of war has become rare, the gap between diplomatic and overt military dispute resolution has

Downloaded by [United States Military Academy] at 08:07 15 January 2015

never been wider. In addition, the growing importance of cyber as a domain has placed it at the forefront of covert actions.

Every state has a different definition for covert action, yet the basic premise holds across nations. Where covert action differs significantly between states is in the legal frameworks associated with its use.

The Use of Covert Action

Covert action is not a rare occurrence. Gregory Treverton earlier identified more than 900 operations at various levels between 1951 and 1975 in which the "silent option" was used.[24] Loch Johnson has indicated that covert action has been used very differently by each presidential administration.[25] Not only do the aggregate number of covert actions vary from President to President, the intensity of those actions varies as well. More recently, the administration of President Barack Obama has sanctioned the use of hundreds of drone strikes around the world among other covert actions.[26] The question still remains, why is covert action used?

In his 1989 study, Johnson cited Henry Kissinger as providing a succinct logic for covert action. According to Kissinger: "We need an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot operate."[27] As James Fearon described the international bargaining range, a middle area frequently exists in which bargaining simply becomes too difficult. This is what Kissinger referred to as the "grey area." Belaboring the point is important because it provides nuance to the concept of covert action. Parsing out what covert action is makes possible the contextualization of modern covert acts. Practitioners and scholars have helped frame the rationale for covert action and define its broader boundaries. Their views often provide contradictory frameworks within which to understand covert action.

Practitioner Duane Clarridge wrote in his memoir:

> Covert action entails special activities, such as political action and paramilitary operations, to advance U.S. foreign policy objectives by influencing events in foreign countries. I believe I concluded at this time that my purpose in life and the reason I was in the CIA was to advance the interests of the U.S. government and the American people abroad.[28]

Practitioner James M. Olson noted in his book on the morality of spying:

> Espionage is a crime in every country, and the United States practices it in almost every country. Covert action, defined as intervening secretly in the affairs of foreign countries, is a blatant violation of international law.[29]

Downloaded by [United States Military Academy] at 08:07 15 January 2015

Practitioner Theodore Shackley in his memoir provided this advice:

> Covert action operations can be as deceptively peaceful as a letter-writing campaign or as flagrantly violent as a guerrilla uprising. In every case, though, the instigating government must make at least a token effort to hide its hand.[30]

Intelligence scholar Loch Johnson has quoted former Congressman and Secretary of Defense Les Aspin as saying:

> [C]overt actions should be as consistent as possible with the moral character of the American public, so that if some action becomes public, it would not be terribly embarrassing to the government of the United States because it is not something most Americans would consider immoral.[31]

President Richard M. Nixon explained:

> Overt economic or military aid is sometimes enough to achieve our goals. Only a direct military intervention can do so in others. But between the two lies a vast area where the United States must be able to undertake covert actions. Without this capability, we will be unable to protect important U.S. interests.[32]

Each offered a perspective on the value of covert action, ranging from the practical to the moral and legal. While varying on the moral and legal ramifications of covert action, each to some extent acknowledged that covert action fills a necessary gap in foreign policy. Yet, a gap remains in defining what constitutes covert action.

Determining Covert Action's Value

Even then, defining covert action is less difficult than assigning its value. In defining covert action, a rigorous framework should be provided within which to understand it. Beneficial is Loch Johnson's outline of four broad categories of covert action: Propaganda, Political Covert Action, Economic Covert Action, and Military Covert Action. Each title is somewhat self-defining. Johnson identified a scale or ladder of covert action. Figure 2 is a modified version of Johnson's scale of covert action.[33] The changes herein made to his original ladder include critical infrastructure destruction, pinpointed digital actions against combatants, critical infrastructure degradation/denial, and computer network exploitation. Each addition adds a host of potential actions emanating from cyber domain that fall distinctly within the ladder at various locations.

Utility is determined, not by the type of covert action, but rather by its expected effect on the intended target in relationship to the possible costs associated with failure. That said, the further up the ladder of covert

Downloaded by [United States Military Academy] at 08:07 15 January 2015

Threshold Four: Extreme Options
34 Use of WMD
33 Major Secret Wars
32 Critical Infrastructure Destruction
31 Assassination
30 Small-scale coup d'état
29 Major economic dislocations; crop, livestock destruction
28 Environmental alternatives
27 Pinpointed covert retaliations against non-combatants
26 Torture to gain compliance for a political deal
25 Extraordinary rendition for bartering
24 Major hostage rescue attempts
23 Pinpointed digital actions against foreign combatants (non-civilians)
22 Sophisticated arm supplies
Threshold Three: High Risk Options
21 Massive increases of funding in democracies
20 Critical infrastructure degradation/denial
19 Small-scale hostage rescue attempt
18 Training of foreign military forces for war
17 Limited arms supplies for offensive purposes
16 Limited arms supplies for balancing purposes
15 Economic Disruption without loss of life
14 Information Communications Systems Disruption without loss of life
13 Modest funding in democracies
12 Massive increases of funding in autocracies
11 Large increases of funding in autocracies
10 Disinformation against democratic regimes
9 Disinformation against autocratic regimes
8 Truthful but contentious propaganda in democracies
7 Truthful but contentious propaganda in autocracies
Threshold Two: Modest Intrusions
6 Low-level funding of friendly groups
5 Computer Network Exploitation
4 Truthful, benign propaganda in democracies
Threshold One: Routine Operations
3 Truthful, benign propaganda in autocracies
2 Recruitment of covert action assets
1 Support for routine sharing of intelligence

Figure 2. The Covert Action Ladder.[34]

Downloaded by [United States Military Academy] at 08:07 15 January 2015

action a nation precedes, the greater the ramifications for failure and conversely the potential for great gain. A national leader with serious commitments is unlikely to be assuaged by the mild covert actions available at the lower thresholds. But, the consequences of an extreme covert action, such as a failed state-sponsored coup d'état, could lead to overt war and thus could portend a great deal of negative utility. Covert actions must be carefully tailored to meet the need and risks of a given situation. Obviously, the most basic, lower-level thresholds pose much less risk than those at higher thresholds of action. They also are likely to offer less reward. Yet, a series of actions with little independent political utility

might be more effective and result in a combined utility greater than a single risky operation having a one-time possibility for a higher utility payoff.

Cyber actions fall at various levels, ranging from rather benign information operations designed to sway public opinion to extreme options of critical infrastructure destruction through cyber means. The potential gain from each operation is independent. Seeing how cyber operations can influence a state and its citizens is not difficult. Tests such as Aurora at the Idaho National Laboratory or the failure of SCADA systems in the 2009 Metro-rail accident in Washington, D.C. illustrate the potential damage that can occur or be caused through the cyber domain.[35] These are not isolated incidents. Beyond the sheer number of accidents that occur due to malfunctioning code or systems lies a plethora of exploits capable of rendering many of these same services inoperable, or worse result in spillover damages.

The threshold of covert action(s), as in any diplomatic or military setting, must be calibrated to achieve the greatest benefit at the lowest cost. Temporal problems aside, in attempting to bridge the gap many tools can be used to alter the bargaining range between states, among them is covert cyber action. Overt forms of signaling include threats or the imposition of economic sanctions.

The motivation and utility for conflict are variable factors that lead states to engage in hostilities rather than negotiate. Although many theories analyze the motivations for conflict, ranging from misperceptions to outright irrationality, the reality behind the motivation for most major state-on-state wars and the utility assigned to those wars arguably occurs because of an information gap between the potential belligerents. This gap can be, and has been, altered by covert actions of states. Because covert action can fill the gap between war and diplomacy it can achieve political utility.

Positive utility through covert action occurs when narrowing the range of policy options minimizes issue indivisibilities, hidden information, or when it changes the leadership of an opponent state. Following are two examples of the use of covert cyber action to achieve positive utility in the gap between public diplomacy and outright war.

Syria 2007

Although Israel's attack on Syria's nuclear facility is often considered controversial and prone to hearsay, synthesizing the potential ramifications of a combined cyber, kinetic attack is useful. In September 2007 multiple Israeli Air Force bombers flew undetected along the Syrian–Turkish border. The next day public accounts and satellite imagery showed the remains of what was purported to be a nuclear weapons development site being built by the Syrians in cooperation with North Korea. All the more amazing about this attack is that the sophisticated Russian-made

Downloaded by [United States Military Academy] at 08:07 15 January 2015

Tor-M1 and S-300/SA-10 surface to air missiles (SAMs) were not activated, and not a single Syrian fighter plane was scrambled to intercept the Israeli force.[36]

Multiple intelligence officials, ranging from Richard Clarke to Joel Brenner, have arrived at the same conclusion: The Israelis engineered a cyber attack to spoof the Syrian air defense systems. This cyber attack gave the invading Israeli bombers clear skies in which to engage their target.[37] No accurate equivalent for this type of attack can be found in the annals of conventional military operations. This was not an attempt to obfuscate an operation; instead, it provided the equivalent of an invisibility cloak. This type of attack is a dual covert, overt attack. Once the bombs were dropped on the facility the attribution and covert nature of the attack was eliminated. Reducing the number of potential hostile perpetrators down to the only plausible one eliminated the covert nature of the attack. But Israel's ability to conduct the attack was predicated on the covert operation that shifted the tactical advantages wholly in its favor. Furthermore, this covert operation had likely been in the planning and even implementation phases for a long period of time prior to the actual overt air sortie.

Does this type of attack alter the bargaining range and mitigate an overt war? Independently, the cyber attack in this instance was not capable of gaining utility to alter an opponent's policy position. Without the cyber attack, the probability for all-out overt conflict would have increased dramatically. The covert cyber operation's utility is in this instance defined in its ability to act as a force multiplier. This then makes the utility of the operation a function that includes the use of cyber. By facilitating the engagement of a weapons development program, the cyber attack increased the vulnerability of the Syrian regime, mitigated the need for other tools to alter the bargaining range, eliminated an indivisible issue, and alleviated an information asymmetry.

Could the Israelis have conducted the attack without the use of the cyber attack? The historical example of Operation Opera in Iraq in 1981 indicates it was a distinct possibility. But the differences between Iraq and Syria are plain. Israel and Iraq do not share a border, while Israel and Syria do. The mere proximity of the two countries would indicate an increased probability for war had Israel engaged in a similar attack that had not been facilitated through covert means.

To claim that the combined attack eliminated an indivisible issue, Syria's development of nuclear capabilities, is reasonable. Regardless of whether the attack fell within the bargaining range where covert action is most effective, it was both *ex-ante* and *ex-post* efficient from the Israeli perspective. They were able to eliminate a potential threat and neither side suffered casualties (although the North Korean suppliers did). By

Downloaded by [United States Military Academy] at 08:07 15 January 2015

eliminating the nuclear facility, the Israelis forced Syria toward a more favorable policy position, thereby indicating a positive utility.

Stuxnet 2009

This second mini-case is a pure instance of covert cyber action garnering utility. In 2010 Iran admitted experiencing problems with its nuclear enrichment facilities at Natanz. The *Wall Street Journal* reported that Iran was the victim of a highly sophisticated cyber attack.[38] Other news organizations followed up with stories claiming that the malicious software specifically targeted Siemens systems in configurations typically used for centrifuges designed to enrich uranium. The result was a significant delay in Iran's production capabilities of Highly Enriched Uranium (HEU).[39] Software security company Symantec followed up on the Stuxnet story by issuing a report detailing the malicious software.[40] The Symantec report indicated that the virus exploited at least four previously unknown zero-day vulnerabilities.[41] These news reports and corporate analyses of the software combined to provide a unique picture of one of the first significant cyber covert actions.

New York Times reporter David Sanger revealed in the summer of 2012 that Stuxnet was part of a highly classified series of covert cyber actions taken against Iran called "Olympic Games."[42] Sanger indicated that the goal was to affect the very nature of the Iranian nuclear development without the hands of the United States or Israel being seen.[43] Contained within high-level policy discussions were the associated benefits of a covert operation that alleviated the need for overt conflict. This incident provides direct evidence of the use of cyber specifically intended as a covert act against a state.

Bridging the Gray Area

The Stuxnet virus worked across the gray area that underlies Fearon's rational explanations for war. Covert cyber actions against Iran resulted in *ex-ante* and *ex-post* efficiency. A poorly kept secret has long been that Iran has harbored non-civilian nuclear intentions since the fall of the Shah in 1979. The Iranians have a clearly stated desire for a civilian nuclear program, while working to conceal their non-civilian program in tandem. This dual goal has created information asymmetry between Iran and the international community. The information gap between what is and is not acknowledged by Iran engenders distrust between that country and many Western nations. Frequent calls by former President Mahmoud Ahmadinejad (and others) in the Tehran leadership for the obliteration of Israel heightened the trepidation surrounding Iran's potential for acquiring nuclear weapons.[44]

Downloaded by [United States Military Academy] at 08:07 15 January 2015

The situation prior to the use of the Olympic Games tactic was complex. Intelligence officials knew that Iran was developing HEU, and they knew that Iran was within a few years of reaching weapons-grade HEU, yet Tehran refused to acknowledge either of these two facts. This left both the United States and Israel with two highly provocative choices. First, continue to engage Iran through the International Atomic Energy Agency (IAEA) and other back channels and hope that deterrence would work, or second, use kinetic weapons to destroy/damage Iran's HEU development capabilities and risk starting a war. Iran's support of terrorist organizations, including Hezbollah and Hamas, made the first option highly unattractive to Israel and the United States. The second option was particularly unattractive to the United States as it attempted to withdraw from two ongoing wars. This left the international community, Israel, and the United States in a quandary. Israel wanted to eliminate what it perceived as a threat, and the United States didn't want to engage in still another war. The information asymmetries persisted because Iran continued to hide its nuclear enrichment facilities. Covert cyber action offered a third alternative.

Effects on Policy

Although scholars often focus on Stuxnet's functional characteristics, its resultant effect on government policies has had the greatest impact. Olympic Games by some accounts delayed or slowed Iranian HEU production by as much as three years. In addition, it sowed the seeds of doubt in the Iranian engineers' minds about the quality of their enrichment operations, thereby slowing the development process and requiring them to constantly second-guess their development efforts. The resulting delay also reduced the need for immediate kinetic, meaning bombing, attacks against Iranian facilities and thwarted the possibility of a regional conflict in the short term. The damage to the program and the inadvertent release of the malicious code eliminated virtually all information asymmetries relating to the true nature of the programs.

Stuxnet, as a covert cyber action, generated positive utility in several ways: first, it delayed a policy drift away from the status quo. Second, it forced out into the open the primary causal mechanism for a potential conflict. By alleviating this information asymmetry it facilitated another tool of state economic sanctions. The exposure of Iran's nuclear enrichment capabilities arguably impressed upon the international community the need to enhance economic sanctions against them. Third, it increased both *ex-ante* and *ex-post* efficiency. Stuxnet, falling between both ends of the overt spectrum, provided a middle range within which to achieve political objectives.

By mitigating *ex-post* inefficient war, at least in the short-term, and by creating a space in which to use other tools of state, Stuxnet can be

Downloaded by [United States Military Academy] at 08:07 15 January 2015

regarded as a highly successful covert cyber action. Stuxnet was covert because the United States and Israel maintained plausible deniability until Sanger's revelations in his 2012 book.

Confront and Conceal

Had the virus had merely identified Iran's movement towards HEU, it would have increased the need for overt armed conflict. But because Stuxnet delayed the production of HEU, it provided time for overt diplomacy to have a chance at mitigating the need for conflict.

The U.S.–Israeli operation was not perfect. Stuxnet did not have a self-delete function and was eventually released into the wild. Although it did not adversely affect other systems, due to its programing structure, it would have been of greater benefit had the operation remained completely secret.[45] At present, what, if any, costs might be associated with a loss of anonymity by the United States and Israel remain uncertain.

THE UTILITY OF COVERT CYBER ACTION

Utility and covert actions are not mutually exclusive. Nor do both sides to a dispute need to be aware of the other's actions for one side to gain or lose in utility. Although coalitions and partnerships in covert action can aid in the development of better weapons and operations, the resultant utility is calculated independently for each state, so long as the action remains covert. This independence of utility from covert acts differs from overt conflict. Covert cyber action can occur with no monotonic decline in the power relations of states because geographical distance is not a factor. The utility benefit to each state is calculated solely as it pertains to the movement of the instigating party in relation to its target. Similarly, two states might be able to mutually develop a more powerful cyber weapon, but because the weapon is effectively non-excludable, as code for a virus can easily be copied, the power scores of each state are affected only insofar as they alter their ability to inflict damage. The defensive aspects of their utility calculus remain largely unchanged because in-kind cyber retaliation against one nation is unlikely to affect the other.

For too long scholars have focused on the overt world of utility and ignored the bargaining range affected by actions in the shadows of international relations. By citing a broad range of literature, and by bringing in statements from scholars, politicians, and practitioners, I have presented evidence that covert cyber action can be examined using expected utility theory. Covert action is a tool of rational states. While leaders can abuse this tool, the states, acting as unitary actors, can determine the utility of covert actions whether they are conventional or

Downloaded by [United States Military Academy] at 08:07 15 January 2015

cyber covert acts. Furthermore, covert action arguably works best in what James Fearon defined as the bargaining range between states.

Covert action so often falls to the sidelines of international relations because of its moral and ethical considerations. Additionally, the inability to gather current evidence on the state of covert action dissuades academics from rigorous study this "silent option" and its implications. Although the gap between overt diplomacy and overt war can be large, turning attention away from this bargaining range is to ignore the real world tools being used to affect it. Covert action can and does play a role in the space between diplomacy and war. The utility of covert action is derived from its ability to alter the policy relationships of states in international relations and achieve tangible benefits to a government.

Downloaded by [United States Military Academy] at 08:07 15 January 2015

REFERENCES

[1] Albert Einstein and Alice Calaprice, *The New Quotable Einstein* (Princeton, NJ: Princeton University Press, 2005), p. 173.

[2] James D. Fearon, "Rationalist Explanations for War," *International Organization,* Vol. 49, No. 3, 1995.

[3] James E. Cartwright, ed. "Joint Terminology for Cyberspace Operations," U.S. Department of Defense, 2010.

[4] James D. Fearon, "Rationalist Explanations for War."

[5] "What are Information Operations," Cyberspace and Information Operations Study Center, at http://www.au.af.mil/info-ops/what.htm

[6] *Ibid.*

[7] Herbert A. Simon, "Human Nature in Politics: The Dialogue of Psychology with Political Science," *The American Political Science Review,* Vol. 79, No. 2, 1985, p. 294.

[8] James D. Fearon, "Rationalist Explanations for War."

[9] See Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979) for discussions on anarchy; see Michael W. Doyle and Stephen Macedo, *Striking First: Preemption and Prevention in International Conflict* (Princeton, NJ: Princeton University Press, 2008) for why preemptive war is not a rational path for war instigation; see Bruce Bueno de Mesquita, "An Expected Utility Theory of International Conflict," *The American Political Science Review,* Vol. 74, No. 4, 1980 for a discussion on utility XE "utility" and conflict.

[10] Bruce Bueno De Mesquita, *The War Trap* (New Haven, CT: Yale University Press, 1981), p. 31.

[11] James D. Fearon, "Rationalist Explanations for War," p. 390.

[12] *Ibid.*, p. 404.

[13] *Ibid.*, p. 382.

[14] See Arthur Stein, "Coordination and Collaboration: Regimes in an Anarchic World," in David A. Baldwin, ed., *Neorealism and Neoliberalism: The Contemporary Debate* (New York: Columbia University Press, 1993), p. 41.

[15] *Ibid.*

[16] Politics, in *Merriam Webster Dictionary,* 2012.

[17] John Von Neumann and Oskar Morgenstern, *Theory of Games and Economic Behavior* (Princeton, NJ: Princeton University Press, 1944).

[18] Anthony Downs, *An Economic Theory of Democracy* (New York: Harper, 1957).

[19] *Ibid.*, p. 36.

[20] *Ibid.*

[21] Irving L. Janis and C. R. M. Productions, "Group Dynamics Groupthink" (New York: McGraw-Hill Films: Produced by CRM Educational Films, 1973); Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica,* Vol. 47, No. 2, 1979.

[22] Robert Grafstein, "Rationality as Conditional Expected Utility Maximization," *Political Psychology,* Vol. 16, No. 1, 1995.

[23] "National Security Act of 1947," *National Security Act of 1947* (2009).

[24] Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987), p. 12.

[25] Loch K. Johnson, *America's Secret Power: The CIA in a Democratic Society* (New York: Oxford University Press, 1989), p. 103.

[26] David Rohde, "The Obama Doctrine: How the President's Drone War is Backfiring," *Foreign Policy*, March/April, 2012.

[27] Loch K. Johnson, *America's Secret Power: The CIA in a Democratic Society*, p. 17.

[28] Duane R. Clarridge and Digby Diehl, *A Spy for All Seasons: My Life in the CIA* (New York: Scribner, 1997), p. 42.

[29] James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (Washington, DC: Potomac Books, 2006), digital location 791.

[30] Theodore Shackley and Richard A. Finney, *Spymaster: My Life in the CIA* (Dulles, VA: Potomac Books, 2005), digital location 658.

[31] Loch K. Johnson, *The Threat on the Horizon: An Inside Account of America's Search for Security After the Cold War* (Oxford and New York: Oxford University Press, 2011), digital location 10752.

[32] Quoted in William J. Daugherty, *Executive Secrets: Covert Action and the Presidency* (Lexington: University Press of Kentucky, 2004), p. 9.

[33] Loch K. Johnson, *Secret Agencies: U.S. Intelligence in a Hostile World* (New Haven, CT: Yale University Press, 1996), pp. 62–63. See also: Loch K. Johnson, "On Drawing a Bright Line for Covert Operations," *The American Journal of International Law,* Vol. 86, No. 2, 1992.

[34] *Ibid.*

[35] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011); Christopher Conkey, Elizabeth Williamson, and Cam Simpson, "Washington Metro Delayed Upgrades," *The Wall Street Journal*, 24 June 2009.

[36] David A. Fulghum to *Aviation Week*, 2007, at http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog:27ec4a53-dcc8–42d0-bd3a-01329aef79a7&plckCont

Downloaded by [United States Military Academy] at 08:07 15 January 2015

roller=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%253a27ec4a53-dcc8–42d0-bd3a-01329aef79a7Post%253a2710d024-5eda-416c-b117-ae6d649146cd

[37] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Ecco, 2010).

[38] Vanessa Fuhrmans, "Virus Attacks Siemens Plant-Control Systems," The *Wall Street Journal–Eastern Edition,* 256, no. 18, 2010.

[39] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times,* 2011.

[40] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response, 2011.

[41] *Ibid.*

[42] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012), p. 8.

[43] *Ibid.*

[44] Associated Press, "Iran: Israel's Zionist Regime 'an Insult to Humanity,'" *The Guardian,* 17 August 2012, at http://www.guardian.co.uk/world/2012/aug/17/iran-israel-zionist-insult-humanity

[45] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*.

Downloaded by [United States Military Academy] at 08:07 15 January 2015