This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Crisis and Escalation in Cyberspace

Martin C. Libicki

Prepared for the United States Air Force

PROJECT AIR FORCE

The research described in this report was sponsored by the United States Air Force under Contract FA7014-06-C-0001. Further information may be obtained from the Strategic Planning Division, Directorate of Plans, Hq USAF.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-0-8330-7678-6

Published 2012 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

Background

The chances are growing that the United States will find itself in a cybercrisis—the escalation of tensions associated with a major cyberattack, suspicions that one has taken place, or fears that it might do so soon. By *crisis*, we mean an event or events that force a state to take action in a relatively short period of time or face the fraught consequences of inaction. When they fear that failure to act leads to war or a great loss of standing, states believe they must quickly decide whether to act.[1] When we use the term *cyberattacks*, we refer to what may be a series of events that start when systems are penetrated and may culminate in such events as blackouts, scrambled bank records, or interference with military operations.

The basis for such a forecast is twofold. First, the reported level of cyberincidents (most of which are crimes or acts of espionage) continues to rise. Second, the risks arising from cyberspace are perceived as growing more consequential, perhaps even faster.

[1] Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis*, Baltimore, Md.: Johns Hopkins University Press, 1981, pp. 7–12, has a good discussion of the definition of *crisis*.

Purpose

The genesis for this work was the broader issue of how the Air Force should integrate kinetic and nonkinetic—that is, cyber—operations.[2] Central to this process was careful consideration of how escalation options and risks should be treated, which, in turn, demanded a broader consideration across the entire crisis-management spectrum.

To put the material on escalation into a broader context, we preface it with an examination of appropriate norms for international conduct with a focus on modulating day-to-day computer-network exploitation and building international confidence (Chapter Two). Chapter Three covers narratives, dialogue, and signals: what states can and should say about cybercrises. A state that would prevail has to make a clear story with good guys and bad guys without greatly distorting the facts (beyond their normal plasticity).

Chapter Four broaches the subject of limiting an open conflict. If cyberwarfare is clearly subordinate to violent combat (both in the sense that it is overshadowed by violent conflict and in the sense that it can be instrumental to violent conflict while the reverse is much less likely to be true), then the control of the latter is likely to dominate the former. But if cyberwar takes place without violent accompaniment or if the effects of cyberattack are global while the violence is local, then the management of cyberconflict becomes more important.

The penultimate chapter then builds from that material to discusses strategic stability. Primarily, it argues that crises are less likely to emanate from the unavoidable features of cyberspace than they are to arise from each side's fear, putatively exaggerated, of what may result from its failure to respond. Chapter Six asks and answers the question whether cybercrises can be managed.

---

[2] Nonkinetic operations can also be other than cyber, such as psychological or information operations, but the study team focused on cyber.

Avoiding Crises by Creating Norms

Norms—accepted standards of behavior—can help avert crises arising from misperception, mistakes, or misattribution. Obligations to assist investigations of cyberattacks, when met, can help build mutual confidence. Those that persuade states to dissociate themselves from nonstate hackers can make it harder for targets of cyberattack to accuse a given state of being complicit in what might have been criminal attacks. Renouncing espionage to steal intellectual property can help reduce certain tensions associated with the frictions of international trade. But norms are no panacea: Some of what the United States might ask others to do—such as control the bots that spew spam to the rest of the world—are difficult for the United States itself to do.

Norms to govern state behavior in peacetime may be useful even if unenforceable. They put nations on record against certain behaviors. Even if states sign up while harboring reservations or maintaining a cynical determination not to comply, others—such as a nation's own citizens or whistleblowers who balk when asked to act contrarily to norms—may be there to remind states to obey the constraints to which they agreed.

Norms that govern the use of cyberattacks in wartime may also be useful, but enthusiasm about their beneficial effect should be tempered. A state can vow to limit its attacks to military targets, react proportionally to provocation, and avoid deception only to find out that the poor correspondence between intent and effect (and perception) in cyberspace means that it did no such thing.

Narratives, Dialogues, and Signaling

The inherently secret, often incomprehensible, and frequently ambiguous nature of cyberoperations suggests that what actually happened can be overshadowed by the narratives that are used to explain events—especially if the focus on cyberevents is not overwhelmed by the subsequent violence of war. Narratives are made up of the stories that people, organizations, and states tell about themselves to others as a way of

putting events in a broader and consistent context and justifying their attitudes and actions.

Conflicts, to be sure, have always needed explanation, but perhaps nowhere more so than for cyberwar. Cyberoperations lack much precedent or much expressed declared policy on which to rely. The normal human intuition about how things work in the physical world does not always translate effectively into cyberspace. Finally, the effects, and sometimes even the fact, of cyberoperations can be obscure. The source of the attacks may not be obvious. The attacker must claim them, or the defender must attribute them. Even if the facts were clear, their interpretations are not; even when both are clear, decisionmakers and opinionmakers may not necessarily understand.

Today, the level of cyber knowledge, much less expertise, in governments is quite low. This will change, but only slowly. As people gain savvy about cyberspace, narratives about incidents necessarily must become more sophisticated and nuanced. Until then, states, nonstate actors, and partisans on all sides have a great opportunity to make something of nothing or vice versa. If cyberwar becomes more consequential, look for states to avail themselves of such opportunities more often. Narratives become tools of crisis management.

Part of the strategy of interpretation is concocting narratives in which events take their designated place in the logical and moral scheme of things: We are good, you are bad; we are strong and competent, unless we have stumbled temporarily because of your evil. Alternatively, the emphasis can be on systems: how complex they are, how easily they fall victim to accident or malice, the difficulty of determining what happened to them, the need to reassert competence, the importance of one network's or system's stability to the stability of all networks and systems. Within wide bands of plausibility, narratives are what states choose to make them.

Dialogue may be needed to manage crises in which incidents arise unrelated to ostensible military or strategic moves by the alleged attacker: If the attribution is correct, what was the motive? The accused state may, alternatively or sequentially, claim that it was innocent, that the attackers did not work at the state's behest (even if they are state employees), that the incident was an accident, that it was nothing

unprecedented, or that it really signified nothing larger than what it was. The accusing state (that is, the victim of the cyberattack) may reject these claims, find a way to verify them (e.g., if the accused state dissociates itself from the attackers, is it also prepared to act against them?), or conclude that it must live with what happened. In some cases, one state takes actions that are within the bounds of what it thinks it can do, only to find that its actions are misread, misinterpreted, or taken to be a signal that the other state never intended to send. Key to this analysis is each side's perception of what the incidents in question were trying to achieve or signal (if anything).

Signals, by contrast with narratives, supplant or supplement words with deeds—often, indications that one or another event is taken seriously and has or would have repercussions. Signaling is directed communication, in contrast with narratives, which are meant for all. Signals gain seriousness by indicating that a state is taking pains to do something; costliness gives signals credibility.

Signals, unfortunately, can be as or more ambiguous when they take place or refer to events in cyberspace than they are when limited to the physical world. For example, the United States recently established U.S. Cyber Command. What might this convey? It could signal that the United States is prepared. It could also signal that it is afraid of what could happen to its own systems. Alternatively, it could signal that it is going to be more aggressive. Or it could indicate some combination of those things. Hence the role of narratives—such as one that emphasizes, for instance, that a particular state is fastidious about rule of law. They are an important complement to signals and perhaps an alternative or a substitute way for others to understand and predict a state's actions.

Escalation Management

Possibilities for escalation management, once conflicts start, must assume that quarreling states would prefer less disruption and violence versus more of it—once they make their points to each other.

The escalation risks from one side's cyberoperations depend on how the other side views them. Because phase 0 operations—preparing the cyberbattlefield by examining potential targets and implanting malware in them or bolstering defenses—tend to be invisible, they should carry little risk. Yet, if they are revealed or discovered, such actions may allow the other side to draw inferences about what those that carried them out are contemplating. Operational cyberwar against targets that are or could be hit by kinetic attacks ought to be unproblematic—unless the other side deems cyberattacks particularly heinous or prefatory to more-expansive attacks on homeland targets. Strategic cyberwar might well likely become a contest of competitive pain-making and pain-taking that is inherently escalatory in form—even if no kinetic combat is taking place.

Tit-for-tat strategies can often be a way to manage the other side's escalation: "If you cross this line, so will I, and then you will be sorry." However, in the fog of cyberwar, will it be obvious when a line is crossed? As noted, the linkages between intent, effect, and perception are loose in cyberspace. Furthermore, if lines are not mutually understood, each side may climb up the proverbial escalation ladder certain that it crossed no lines but believing that the other side did. Assumptions that each side must respond at the speed of light could exacerbate both sides' worst tendencies. In reality, if neither side can disarm the other, then each can take its time deciding how to influence the other.

Third-party participation may well be a feature of cyberspace because the basic tools are widespread, geographical distance is nearly irrelevant, and the odds of being caught may be too low to discourage mischief. A problematic third party might be a powerful friend of a rogue state that the United States is confronting. If the powerful friend carries out cyberattacks against U.S. forces or interests, the United States would have to consider the usefulness of responding to such attacks. Even in symmetric conflicts, the possibility of third-party attacks should also lend caution to responses to escalation that look as if they came from the adversary but may not have. Because escalation management entails anticipating how the other side will react to one's actions, there is no substitute for careful and nuanced understanding of other states. Local commanders are more likely than remote ones to

have such understanding; paradoxically, however, the former do not currently exercise much command and control (C2) over cyberwarriors.

Strategic Stability

With all these concerns about managing cybercrises, it may be worthwhile here to step back and ask whether the existence or at least possibility of cyberwar threatens strategic stability. The best answer is both no and yes: no in that the acts that make nuclear instability an issue do not carry over to cyberspace (attacks meant to temporarily confound conventional forces, as noted, aside), and yes in that other factors lend instability to the threat of the use of cyberwar.

Why the no? First, nuclear weapons themselves limit the existential consequences of any cyberattack. A nuclear-armed state (or its allies) might yield to the will of another state, but it cannot be taken over except at a cost that far outweighs any toll a cyberattack could exact. Cyberattacks cannot cause a state's nuclear weapons to disappear (Stuxnet merely slowed Iran's attempts to build one), and, although cyberattacks could, in theory, confound nuclear C2, nuclear states tend to bulletproof their C2. Attackers may find it hard to be sufficiently confident that they have disabled all forms of adversary nuclear C2 to the point at which they can then act with impunity.

Equally important is the fact that no state can disarm another's cybercapabilities through cyberwar alone. Waging cyberwar takes only computers, access to the Internet, some clever hackers, and intelligence on the target's vulnerabilities sufficient to create exploits. It is hard to imagine a first strike that could eliminate all (or perhaps even any) of these capabilities. If a first strike cannot disarm and most effects induced by a cyberattack are temporary, is it really that destabilizing?

Furthermore, cyberconflict does not lend itself to a series of tit-for-tat increases in readiness. During the Cold War, an increase in the readiness of nuclear forces on one side prompted a similar response from the other, and so on. This follows because raising the alert level is the primary response available, the advantage of the first strike is great, and preparations are visible. None of this applies to cyberwar, in

which many options are available, what happens tends not to be visible, and first strikes cannot disarm. In addition, during the Cold War, making nuclear strike capabilities invulnerable was perceived as enormously destabilizing because it rendered the opponent's nuclear arsenal harmless by destroying it. But, in large part because cyberdefenses will never be perfect, they pose no such threat and thus are not inherently destabilizing.

Arms races have traditionally fostered instability. Such a race already exists in cyberspace between offense and defense. Offense-offense races are less plausible. There is no compelling reason to develop an offensive weapon simply because a potential adversary has one. It is hard to know what others have, and the best response to an offensive cyberweapon is to fix the vulnerabilities in one's own system that allow such cyberweapons to work.

However, the subjective factors of cyberwar do pave paths to inadvertent conflict. Uncertainties about allowable behavior, misunderstanding defensive preparations as offensive ones, errors in attribution, unwarranted confidence that cyberattacks are low risk because they are hard to attribute, and misunderstanding the norms of neutrality are all potentially sources of instability and crisis. Examples can include the following:

- Computer network exploitation—espionage, in short—can foster misperceptions and possibly conflict. Normally, espionage is not seen as a reason to go to war. Everyone spies on everyone, even allies. But then one side tires of having its networks penetrated; perhaps the frequency and volume of exploitation crosses some unclear red line; or the hackers simply make a mistake tampering with systems to see how they work and unintentionally damage something.
- One side's defensive preparations could give the other side the notion that its adversary is preparing for war. Or preparing offensive capabilities for possible eventual use could be perceived as an imminent attack. Because much of what goes on in cyberspace is invisible, what one state perceives as normal operating procedure, another could perceive as just about anything.

- The difficulties of attribution can muddle an already confused situation. Knowing who actually did something in cyberspace can be quite difficult. The fact that numerous attacks can be traced to the servers of a specific country does not mean that that state launched the attack or even that it originated in that country. Or, even if it did originate there, that fact does not mean that the state is complicit. It could have been launched by a cybercriminal cartel that took over local servers. Or some third party could have wanted it to look as though a state launched an attack.

Cyberwar also provides rogue militaries with yet another way to carry out a no-warning attack, another potential source of instability. If an attacker convinces itself that its efforts in cyberspace cannot be traced back to it, the attacker may view an opening cyberattack as a low-risk proposition: If it works well enough, the attacker can follow up with kinetic attacks, and, if it fails to shift the balance of forces sufficiently, no one will be the wiser. If the attacker is wrong about its invisibility, however, war or at least crisis may commence.

Otherwise, from a purely objective perspective, cyberwar should not lead to strategic instability. However, cyberwar may not be seen as it actually is, and states may react out of fear rather than observation and calculation. An action that one side perceives as innocuous may be seen as nefarious by the other. A covert penetration may be discovered and require explanation. Cyberwar engenders worry. There is little track record of what it can and cannot do. Attribution is difficult, and the difficulties can tempt some while the failure to appreciate such difficulties can tempt others. Espionage, crime, and attack look very similar. Nonstate actors can pose as states. Everything is done in secret, so what one state does must be inferred and interpreted by others. Fortunately, mistakes in cyberspace do not have the potential for catastrophe that mistakes do in the nuclear arena. Unfortunately, that fact may lead people to ignore the role of uncertainty and doubt in assessing the risk of inadvertent crisis.

Conclusions and Recommendations for the Air Force

Cybercrises can be managed by taking steps to reduce the incentives for other states to step into crisis, by controlling the narrative, understanding the stability parameters of the crises, and trying to manage escalation if conflicts arise from crises. Given the paucity of cyberwar to date, our analysis produces more suggestions than recommendations. That noted, an essential first step of cybercrises is to recognize them for what they are, rather than metaphors of what they could be.

As for recommendations, the Air Force can contribute a great deal to assist in cybercrisis management:

- Crisis stability suggests that the Air Force find ways of conveying to others that its missions can be carried out in the face of a full-fledged cyberattack, lest adversaries come to believe that a large-scale no-warning cyberattack can provide a limited but sufficient window of vulnerability to permit kinetic operations.
- The Air Force needs to carefully watch the messages it sends out about its operations, both explicit (e.g., statements) and implicit. To be sure, cyberspace, in contrast to the physical domains, is an indoor and not an outdoor arena. It may thus be hard to predict what others will see about offensive Air Force operations in cyberspace, much less how they might read it. But the assumption that unclassified networks are penetrated and thus being read by potential adversaries may be a prudent, if pessimistic, guide to how potential adversaries may make inferences about Air Force capabilities and intentions.
- If there is a master narrative about any such cybercrisis, it is axiomatic that Air Force operations should support rather than contradict such a narrative. The Air Force should, in this regard, consider how cyberspace plays in the Air Force's own master narrative as a source of potentially innovative alternatives—wisely selected and harvested—to meet military and national security objectives.
- The Air Force should clearly differentiate between cyberwar operations that can be subsumed under kinetic operations and cyberwar operations that cannot be subsumed. The former are unlikely

to be escalatory (although much depends on how such options are perceived) when their effects are less hazardous than a kinetic alternative would be. The latter, however, may create effects that could not be achieved by kinetic operations that, if undertaken, would be universally perceived as escalatory.

- Finally, Air Force planners need a precise understanding of how their potential adversaries would perceive the escalatory aspect of potential offensive operations. Again, more work, with particular attention to specific foes, is warranted. For this purpose (and for many others), the Air Force should develop itself as an independent source of expertise on cyberwar.