Hacking Networks of Terror

Ronald J. Deibert and Janice Gross Stein

War by a Network

That we in North America face a new kind of threat is beyond question. The attacks against the heartland of the United States, its corporate and military icons, and the killing of over 3,000 civilians, mark a watershed in thinking about security. It is almost two hundred years since civilians in North America have been the object of systematic attack, and even longer since the core of the hegemonic power was struck from the periphery. The important analytical and political questions are What kind of threat do we face? What is the appropriate response to that threat? In other words, what are the appropriate ways to think about dealing with a threat from a nonstate actor with no fixed location or permanently defined territorial assets?

President George W. Bush claims that the threat is from "evil doers" who seek to destroy Western civilization. This is a struggle of good against evil, of the forces of darkness against light. These forces of darkness are themselves threatened by the openness, the affluence, and the cultural diversity of postindustrial democratic society. Here, we come close to an argument of a clash of civilizations, even if that clash is not between Islam and the West.[1] Others claim that the attacks are the work of a small, maniacal group of terrorists, unrepresentative of the mainstream of their societies, and isolated in small, disorganized, conspiratorial units. While both analyses capture part of the more complex character of the current threat, neither analysis can stand close scrutiny and the weight of evidence. And, more important, the conceptual language is wrong.

We are in a new kind of struggle, one against a network with global reach. We need to understand who organizes and manages this particular network. And we need appropriate conceptual language to understand what a network is, how it operates, how it thrives, and how it withers, if we are not to misunderstand the threat and misconceive the response.

For those seeking answers to these questions, most theorizing on security--both rationalist and reflective--offers only limited help. Mainstream rationalist approaches to security treat states as unitary, rational actors--billiard balls with hard

Dialog-IO, Spring 2002, pp. 1–14

[1] Huntington 1996.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

outer shells and a sharp division between "inside" and "outside."[2] The group that organized the attacks on the United States, however, is part of a decentralized and transnationally dispersed network of religious extremists. Even if the terrorists are considered to be a "conflict group" equivalent to a state, their decentralized operational structure prevents them from acting in a unitary, rational way with clearly defined preferences that are knowable *ex ante.*[3] One of the characteristics of the terrorist network that organized the attacks was that local units operated with a significant degree of autonomy.

Not only are actor models misleading, but so is the way in which power is conceived by traditional theories of international relations. Realist approaches to international relations treat concentrated military and economic capabilities as the indicators of power.[4] But the military instruments that were employed by the terrorists--hijacked jets as ballistic missiles, public Internet terminals, cell phones, and rental cars--were plucked from the postindustrial fabric of the society that was targeted, rather than developed through a traditional process of national-military industrialization. How does a state "balance" against power assets and material resources that are part of its own society? And how do we theorize about a threat from actors whose capabilities are not only dispersed but also unpredictable, and hence cannot be measured?

"Reflective" or "critical" theories, on the other hand, can help decipher and deconstruct the paradigms through which threats to security are defined.[5] They offer little help, however, on how to deal with specific threats once they are identified and agreed upon. Admittedly, reflective approaches to security are forms of "critical," as opposed to "problem-solving," theory.[6] They stand outside the present order and ask how it came to be, while pointing the way toward alternative paths of development for the future. They help develop an understanding of why some threats are given attention and others are marginalized. But they are less useful in developing strategic concepts for a mutually agreed construction of a threat and the appropriate response.

The network as an organizational form and "actor" in world politics requires a different set of conceptual tools than those found in traditional and reflective approaches to world politics. Different tools are required not because networks are new *per se* but because they differ from hierarchical forms of organization, such as states, that are the core unit of analysis in most theories of international relations.

Although networks are often associated with postindustrial society, the network as an organizational form is an ancient practice.[7] Maritime trading networks were common in archipelagos in ancient Greece and the islands that now make up Indonesia. Christian religious scholars based in relatively isolated monasteries of west-

[2] Smith 1999.
[3] Legro and Moravcsik 1999.
[4] Waltz 1979.
[5] Krause and Williams 1997.
[6] Cox 1984.
7Landa 1994.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

ern Europe in the early Middle Ages organized a very effective form of interaction through distributed social networks. Likewise, the Maghrebi traders of the eleventh-century Muslim world employed networks of information exchange.[8] Families, ethnic diaspora groups, and communities around the world can all be seen as variants of social networks.[9] Networks have always coexisted with hierarchical forms of social organization, sometimes prominently, other times submerged, depending on the historical and cultural context.

Nor is the study of networks new. Social network analysis came to prominence in the anthropologist A. R. Radcliffe-Brown's seminal 1940 article, "On Social Structures."[10] Ever since, many sociologists and anthropologists have employed network analysis to understand the linkages between people across domains. In international relations, the concept of the network, if not the formal term, is embedded in the work of functionalist and integration theorists, and in the "cobweb" theory of world order of John Burton.[11] More recently, networks form the core analytic concept of research on transnational advocacy groups and citizen activists.[12]

In this article, we use concepts derived from analyses of networks to investigate networks of terror and to help understand how they operate and function. However, our goal is not only to understand how networks function but also how they can be debilitated. Analyses of networks have examined decay and attrition of networks but have paid less attention to their deliberate disruption.

To help formulate novel strategies for fighting networks, a more experimental approach to language and concept is required, one that sees words and theories not as "mirrors" of reality but rather as "tools" in the service of pragmatic ends.[13] Here, we draw from language and theories associated with warfare and hacking in computer networks to develop a new set of tools to fight networks of terror. We argue that these network-based concepts can provide new and more effective perspectives for military campaigns and intelligence operations against terrorism. At the same time, however, we recognize that all analogies, including those to hacking and network war, have limits. We attempt to make these boundaries clear in our analysis.

The Network as the Basic Form of Postindustrial Organization

We have witnessed the first large-scale violent attack against postindustrial society through its signature form of organization: the network. The network has become the most pervasive organizational image and the dominant form of social organization in postindustrial society. "As a historical trend," observes Manuel Castells, "dominant functions and processes in the information age are increasingly organ-

[8] Greif 1994.
[9] Yarbrough and Yarbrough 1999.
[10] Radcliffe-Brown 1940.
[11] Burton 1972.
[12] Keck and Sikkink 1998.
[13] See Rorty 1979; and Deibert 1997.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

ized around networks. Networks constitute the new social morphology of our societies, and the diffusion of networking logic substantially modifies the operation and outcomes in processes of production, experience, power, and culture."[14] Networks also shape processes of terror and violence. We need to understand the structure of a network, its application, and its resiliency in the face of disruption.

A network is a collection of connected points or nodes, generally designed to be resilient through redundancy. It can be one terminal, connected to the Internet, or one expert communicating with another expert in a common network devoted to a shared problem. Networks, in other words, can be both technological and social. The design of the network determines its resilience, its flexibility, its capacity to expand, and its vulnerability.

The first and still archetypal electronic network is, of course, the Internet. Apparently developed simultaneously by three different sources in the early 1960s--Larry Kleinrock, David Davies, and Paul Baran--the central feature of the Internet is a distributed form of communication without central control.[15] In a distributed network, messages are broken into individual "packets" that then take multiple different paths to reach their destination. Such a mode of transmission allows communication exchanges to continue even if parts of the node are destroyed or inoperative. The network is resilient because of its built-in redundancy; the more nodes are added to the network, the more resilient the network as a whole becomes. Built upon principles antithetical to centralized broadcasting modes of communication, the Internet builds strength through dispersion and multiplication of individual nodes. It is precisely for this reason that centralized forms of political authority find the task of censoring Internet communications so difficult. With the Internet, there is no single node from which all information emanates or passes through. Removing a single node, or even several, will not destroy the network. The network adjusts, reroutes, and reforms as everything from dissident Web sites in China to the trading of MP3 files demonstrates.[16] In the pure model of a network, such as the Internet, eliminating one node of a network does not imperil other nodes.

Global Networks

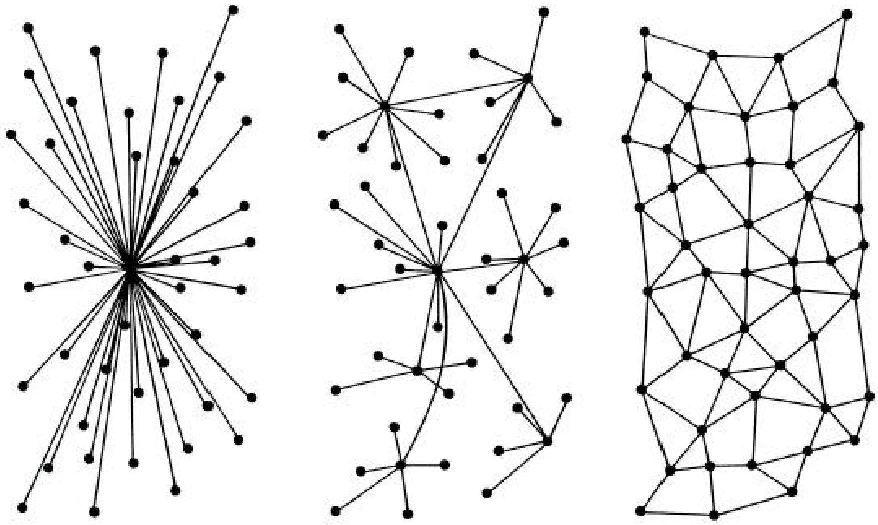
Social networks mirror their electronic counterparts in important ways. They too are highly decentralized, with different leadership branches that operate with a large degree of autonomy. Unlike the tight pyramids of command-and-control political structures, the hallmark of industrial society, networks are "flat," with leaders who are empowered to act with minimal direction and supervision. Using advanced electronic forms of communication, global networks of every kind have multiplied in the last decade: businesses, civil society networks, journalists, scientists,

[14] See Castells 1996, 469; Lipnack and Stamps 1986; and Wellman and Berkowitz 1988.

[15] See Baran 1964; and Hafner 1996.

[16] Deibert forthcoming.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press



a. Centralized/hiearchical b. Decentralized/hierarchical c. Distributed/nonhierarchical

Source: Adapted from Baran 1964.

FIGURE 1. *Centralized/hierarchical, decentralized/hierarchical, and distributred/nonhierarchical networks*

physicians, lawyers, scholars, and environmentalists. These networks differ in how they are organized and, consequently, in their flexibility and resilience.

Most networks generally do not approximate the pure forms (see Figure 1c). Perhaps the most advanced networks can be found in the financial sector, where capital flows relatively seamlessly around the world through integrated electronic trading networks. Another can be found at the opposite end of the political spectrum, among so-called antiglobalization activists.[17] Linked through thousands of Web sites, e-mail lists, and Internet relay chats, citizen activists from around the world have been able to coordinate mass protests at major international events without a hierarchical mode of organization--a capability that seemed to escape the notice of many of the movement's critics who lamented the lack of overall "direction."

Such pure network models are rare, however. A study of global knowledge networks found, for example, that the most successful networks require a center or a "hub," financial support, and a secure environment for the "host," which serves as the temporary organizational focus. There is an element of "place," even if that place is temporary, within which almost all successful networks function.[18] Even

[17] Deibert 2000.
[18] Stein et al., 2001.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

among global financial networks, major urban centers act as crucial, central nodes where financial expertise and personnel are located. It is for this reason that the city of London, for example, occupies such a central role in the global financial economy.[19]

Most social networks build some elements of a "web" into their design, even ones that have major nodes within them. Analysts have suggested, for example, that one of the reasons why complex financial networks were able to resume operations so quickly after the attack on September 11 was that the "corporate headquarters" of many of the firms in the World Trade Center had been moved off-site after the first attack in 1993. Within hours, many had resumed operations because of the redundancy they had built into their information systems. Such redundancy also explains why e-mail traffic continued to move unimpaired on September 11, whereas telephone traffic ground to a halt in the northeastern United States. In the pure model of a network, eliminating one node of a network does not imperil other nodes.

Global Networks of Terror

Global networks of terror bear an uncanny resemblance to their generally benign and productive counterparts. Unlike legitimate global networks, of course, they work in secrecy and through illegitimate practices and violence to advance their political purposes. Often with life-cycles lasting decades, networks of terror thrive on the openness, flexibility, and diversity characteristic of postindustrial society, crossing borders almost as easily as do goods and services, knowledge and cultures. They have global reach, particularly when they can operate within the fabric of the most open and multicultural societies, and through postindustrial organizational forms.

Global networks of terror are enabled by conditions unique to our times. They are conceivable only in a world that is tightly interconnected and in societies that are moving through the processes of postindustrialization. Without global markets and communications, the widespread mobility of people, and multicultural, diverse societies, these networks of terror could not survive, much less succeed.

Many, though not all, "hosts" of networks of terror cling to weak states that can provide a secure environment for the infrastructure and resources they need. They often depend on states for infrastructure, logistics, and training sites. In exchange for the shield the state provides, a network delivers complex political and financial rewards that help a regime to stay in power. An ideal environment for a "host" of a network of terror is a weak or fractured state where a network can provide critically needed assets in exchange for the capacity to operate "in place." Even without a secure physical environment, however, networks can survive; a host can use mobile headquarters, but training, operations, and recruitment become more difficult.

[19] Thrift 1994.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

Who Is this Network?

The existence of Al Qaeda was well known to intelligence analysts and experts on the region long before September 11. Its organizational structure, according to the best available knowledge, in large part resembles a network. It is organized in self-contained nodes that function autonomously, with limited communication and support from the center. Responsibility and decision-making authority are devolved down to the lowest possible level. Unlike open networks, however, each node is unaware of the identities and attributes of others.

The Arabic word *al-Qa'eda* means "base." Historically, the network has had only temporary bases, first in Sudan and then in Afghanistan. It is better described as "a distributed, roaming, nonterritorial network, operating through its combined use of advanced information technologies and traditional *halawa* exchanges."[20] Its nodes communicate through the Internet, funds are transferred through local exchanges with global connections, and its members move freely across the borders of diverse, multicultural societies.

Al Qaeda is also a network of networks. In the last three years it successfully interlinked with other networks led by Egyptian and Algerian dissidents and exiles. The Egyptian network brought a significant increase in the level of operational planning, competence, and logistics to the broader network. As Al Qaeda connects with other networks, it more closely approximates a pure network with very flexible, insulated, and redundant connections.

It does, however, have a center, the equivalent of a small corporate headquarters, and it operates in place. Both these attributes merit some attention. It has a hub, which is led by Saudi and Egyptian dissidents, and is organized as a "corporate" structure, with a *shura* (council). It has a finance committee, a military committee responsible for training and arms purchases, a committee on Islamic study, a media committee, and a travel committee.[21] Leaders are important, but, as in other network structures, not all-important.

It is consequently misleading to personalize the threat as Osama bin Laden, for in this kind of hybrid network-corporate structure, he can be replaced by others were he to disappear. On the other hand, it is also misleading to claim, as some do, that bin Laden is a social construction, that he is the creation of those who seek to personalize and demonize the enemy. His leadership, and his charisma--expressed in part through piety, asceticism, and commitment--has been significant. As in other kinds of social and political organizations, leaders matter in networks. They may matter far less than they do in command-and-control hierarchies, but, even in networks, they still matter. Al Qaeda approximates "a hybrid peer-to-peer network, in which a central source triggers the actions that are carried out by individual

[20] Deibert 2001.

[21] Don Von Natta, Jr., Running Terrorism as a New Economy Business, *New York Times*, 11 November 2001, WK5.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

nodes."[22] Denying the host a secure environment would weaken the network, but the host can find other, less attractive homes. Destroying the center and removing the leader would weaken it even more but would not necessarily disable the network.

Al Qaeda is a network that also functions partly "in place." In its earliest phase of development, it used Sudan as a safe environment for its host. When Sudan expelled bin Laden, he secured his headquarters behind the shield provided by the Taliban in Afghanistan. Here, the network becomes a more familiar and vulnerable organizational form as it organizes training camps, recruits members, and draws on a pool of sympathizers to form a guard around its assets. These assets are potential targets and can be disrupted more easily than a pure network without the organizational apparatus of a corporate headquarters.

Paradoxically, this network organized in postindustrial form is committed to a pre-industrial project of religious monopoly and intolerance. It rejects the postindustrial project even as it adapts its organizational forms and technology to pursue its purpose. Al Qaeda rejects not only postindustrial society but even the hierarchical command-and-control state characteristic of the industrial era. It seeks a return to an earlier community of the faithful uninterrupted by the borders and the divisions of the modern state.

The Challenge of Waging War Against a Network

A struggle against a network is asymmetric: states must fight a global network that is not designed around dominant power centers but is dispersed, flat, and flexible. It is easier, for example, to destroy a weblike structure, with a controlling hub, connected through strands to the points of the web. Destroy the hub, and the web is fatally weakened. Not so with a network. It is for this reason that the concepts and tools of traditional security studies and international relations theory are not much help in this struggle. Networks of terror are nonstate centric, nonterritorial, and largely distributed.

When we think about Al Qaeda as a network, it becomes clear that existing military doctrine, based on concepts of mass-and-maneuver reinforced by heavy strikes from the air, is only the first phase in a much longer struggle. At best, conventional military force can reduce the number of available environments for a host, degrade the capacity of a network to train members, and force the host to become mobile. A military attack to disable those who provide safe haven for the host and the assets of the network is a first but limited response to a network of terror. Its purpose is to deprive Al Qaeda, the host, of the secure geographic environment that the Taliban had provided.

Military attacks, conducted through a command-and-control structure, are designed to be effective against hierarchical state structures with conventionally

[22] John Arquilla and David Ronfeldt, Fighting the Network War, *Wired*, December 2001, 150–61.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

structured and consolidated forces. Here the purpose must be not only to destroy the capacity of this host to find a secure environment in which it can continue to act as a server to the network, but also to disrupt and eventually disable the network. Military doctrine will have to change to decentralize intelligence and command to the lowest possible levels and to provide as much flexibility as possible to give local area commanders the capacity to launch continuous pin-prick attacks from multiple directions to confuse and overwhelm the network.

To return to the analogy of computer networks, they often have more than a single host server. Increasingly, application processing is distributed across a network of hosts that are geographically dispersed. Client work stations, or nodes within the network, access the network for application software and communication with other end-user work stations and with databases that are themselves often distributed in peer-to-peer networks. This analogy is a reasonably good fit with the way those who hijacked commercial flights communicated with nodes of the network that were dispersed. Although the node has no knowledge of which server is supporting which part of the task at any moment, it still needs to have sufficient servers intact and in touch to continue its work.[23]

How then can the capacity of a network be impaired? It is unlikely that networks, organisms with rudimentary central nervous systems, can be completely destroyed. A network has no powerful central "brain" that can be targeted to lead to a "quick kill." Paradoxically, actions designed to "kill" a part of the network identify the part that has been damaged. Like other lower-order organisms, the network then sheds that part and regenerates elsewhere.[24] To destroy the organism, its capacity for regeneration must be gradually degraded, through suffocation and starvation. Similarly, to impair a network's functioning , the capacity of its servers must be degraded, the connections among nodes slowed, and the links between the workstations and the servers interrupted and eventually damaged.

How does this analogy of a computer network translate into a strategy against a network of terror? Reasoning by analogy is one way of creating new conceptual tools. Analogies are not so much "blueprints" for action as they are suggestive lenses through which problems can be reframed. Drawing on analogies from computer network warfare, we suggest three ways in which networks of terror can be "hacked."

[23] We are indebted to Philip Siller for the elaboration of the computer network model to a network of terror.

[24] A good example, mentioned earlier, is the "regeneration" of corporate activity that took place after the attacks on the World Trade Center. Even though the main offices (nodes) of some corporations were destroyed, they could continue their operations from remote locations. Many announced on their Web sites immediately following September 11 that they were operating "business as usual."

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

Multimedia Denial-of-Service Attacks

One of the more prevalent forms of network warfare, used by both states and hackers, has been distributed denial-of-service (DoS) attacks. DoS attacks employ the decentralized character of the Internet to organize an overwhelming and disabling flood of information to attack selected servers. Key to launching a DoS attack is the multiplier effect, which is achieved by controlling "zombie" computers spread throughout the Internet. These kinds of attacks typically use back-door access to computers with fixed IP (Internet protocol) addresses. At prearranged times, the linked zombie computers make repeated requests for fictitious files. The flood of requests for information eventually overwhelms the server's capacity to respond, shutting it down.

Software to organize DoS attacks is widely available on the Internet and its use requires relatively minimal knowledge of network codes and operations. The most well-known DoS attacks have been organized by nonpolitical hackers and crackers targeting large commercial Web sites, such as Yahoo and Ebay. But DoS attacks have also been employed for political ends. One of the first DoS attacks was organized by a pro-Chiapan group called the Electronic Disturbance Theatre based in New York City and directed at the servers of the Mexican government. More recently, DoS attacks against an Internet service provider based in Toronto, Canada, that hosted Web sites of the dissident religious group Falun Gong were traced back to government computers in China.[25]

How can the method of *computerized* DoS attacks be translated into a broader fight against a network of terror? To extend the analogy of a DoS attack to wider domains, the objective would be to overwhelm the nodes of the terrorist network through a multiplier effect, making it more difficult, more time-consuming, and more expensive for users in the field to get what they need from the network's "hosts" and to separate credible, useful information from "noise." More rigorous requirements for documentation, more frequent checks on existing documentation, more frequent checks on compliance with existing regulations would all increase the transaction costs for "users" within the network. This kind of strategy does not necessarily require new powers of enforcement but different approaches to implementing existing regulations.

Rigorous checks could also be complemented by a bombardment or "flooding" strategy, whereby nodes are overwhelmed with data and information flows coming from multiple sources. This kind of strategy both increases the risks for end users and encourages them to communicate with the network for clarification. In the process, they become easier to identify and target and less able to communicate efficiently. Drawing from the analogy of a DoS attack, the key to implementing such a bombardment strategy would be to create a multiplier effect organized through as many dispersed participating nodes as possible.

[25] Deibert forthcoming.

https://doi.org/10.1017/S777777702000018 Published online by Cambridge University Press

Viruses, Trojan Horses, and Worms

Another form of network warfare is the use of viruses, Trojan horses, and worms. These tools are programs or pieces of code that are loaded onto computers without the user's knowledge. Viruses can replicate themselves to the point where they consume all of a computer's available memory and resources. They can also transmit themselves across the network, affecting multiple nodes and users and slowing down the network. Viruses can be extremely disabling, causing random damage to data files as well as compromising private or sensitive information. The "ILOVEYOU" virus of 2000 spread globally within days, costing upwards of $1 billion in lost business, corrupted data, and damage to computers.

In the struggle against terror, analogs to computer viruses can be employed to disable the network. The strategic use of disinformation, misleading signals about possible targets, frequent and at times deliberately misleading messages about information at hand, organized and channelled through multiple media (radio, television, Internet) can make it more difficult for end users to communicate with hosts and visa versa. Such a strategy would also place emphasis on penetrating networks of terror--an admittedly difficult task but one that would greatly facilitate the circulation of misinformation within networks of terror. Misinformation circulated through networks from both inside and outside, like the age-old practice of states' disseminating disinformation, could undermine the credibility of the information circulating through the network and, consequently, hobble its effectiveness.

Disabling Network Nodes

A third strategy is to starve and suffocate the host or the nodes. Depriving the host of a secure environment is only one way to make it more difficult for the host to perform its network function. Careful monitoring of resource transfers can reduce the capacity of the host to function efficiently and in a timely way. When network reaction time is slowed, the user finds it more difficult to complete tasks, and coordination becomes more difficult. Gradually, fewer users qualify as active participants, and the network begins to decline. Networks that lack redundancy, as we have seen, are inefficient. The strategic objective in a struggle against a network of terror is to reduce its redundancy.

Although the defeat of the Taliban has removed Afghanistan as a safe-haven, eliminating at least one of the important servers, there are less costly and risky forms of suffocation that are and should continue to be employed. Coordination and even harmonization of banking regulations among states will help to stifle funding of terrorist networks. Stepping-up international regulation of money laundering would do the same. At the same time, states that provide an attractive "host site" or operational base for terrorists need to be identified and pressured into conforming with the standards of the international community *before* hosts take up residence. Pressure should be put on regimes that "export" or "deflect" their internal political

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

problems to weaker regimes and refuse to open up their political space to legitimate political participation.

All of these strategies depend critically on good intelligence, but our intelligence-gathering systems are not properly configured to wage this battle. Within the intelligence community, the emphasis is on secrecy, compartmentalization, and a command-and-control structure. Forged during the Cold War, intelligence agencies are reflexively insulated from the outside world, both domestically and internationally. The structure is poorly suited to the struggle ahead, as is the emphasis on closed channels and secrecy. To disrupt a network of terror, we will need a reconfigured system of intelligence, one that is decentralized, network based, and able to communicate and confuse in real time. Sharing information across nodes, rather than controlling and limiting information in a hierarchical structure, increases its value and impact.

In the wake of September 11, intelligence agencies around the world have pushed for and in many cases received sweeping new powers to eavesdrop on communication networks in the effort to combat terrorism. While the impetus for these enhanced powers is clear, they may be counterproductive. Increased surveillance from above will not only infringe on civil liberties but also push networks of terrorists further underground, making them harder to track and disrupt. Sophisticated encryption technologies-- now so widespread on the Internet that they are immune to regulation--will be increasingly employed not only by terrorists but also by privacy advocates, civil society actors, and businesses, making the job of surveillance increasingly difficult. What is needed is not so much increased "surveillance from above" but the encouragement of "sousveillance," or "surveillance from below," through public/private partnerships in security and intelligence, both domestically and internationally.[26] Sousveillance will tighten and expand the web of watchers around the world, making it more difficult for networks to operate in secrecy while increasing the flexibility and adaptability of intelligence operations. Citizens as well as states, nongovernmental organizations as well as international institutions will all need to participate. A model of "open-source" intelligence, analogous to the open-source software movement, is more appropriate to the network form.[27] As with open-source software, open-source intelligence thrives on expanding and increasing flows of information and knowledge--the antithesis of the traditional intelligence model. Yet such distributed flexibility is particularly suited to the distributed nature of the threat.

Conclusion

New forms of social organization require new ways of thinking and speaking, particularly in response to threats to security that use these new forms. However, tradi-

[26] Mann, Fung, and Garabet 2001.

[27] For one example of citizen-based, open-source intelligence, see Openflows.org at <http://www.openflows.org/>.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

tional international relations theorizing is notoriously conservative about conceptual experimentation. At a time of significant structural change and crisis, such experimentation needs to be encouraged. While the analogies we have put forward here are tentatively drawn, they suggest a new framework for addressing and responding to network-based terrorist threats. Networklike thinking is suggestive for the reconfiguring of strategies of military and intelligence. It privileges flexibility and local initiative over centralization and command-and-control, openness rather than secrecy, and partnering rather than monopoly. It will require a renewed emphasis not only on electronic but also on human intelligence, a resource neglected for years by intelligence agencies around the world. And, most importantly, it points toward an increasing dispersion, rather than consolidation, of authority in world politics to deal with networks of terror.

Legislators preparing new guidelines for the war against networks of terror would do well to keep these imperatives in mind. Legislation being passed now is reflexively turning to old strategies and methods of surveillance, secrecy, and closure. To respond to the new threat of network terror, however, new tools need to be adopted and employed that deal effectively with the threat while preserving the mix of rights and constraints on power that define liberal democracies around the world. Hacking networks of terror may not be as spectacular as a massive military campaign, but it may be more effective in the long run. Because these hacking strategies depend on targeted covert operations, intelligence and law enforcement cooperation, and the application of legal instruments, there will likely be fewer civilian casualties and highly visible destruction of state infrastructures in host states. In this respect, hacking networks of terror can degrade their capacity to function while minimizing potential resentment and "blowback."

References

Arquilla, John, and David Ronfeldt. 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, Calif.: Rand.

Baran, Paul. 1964. *On Distributed Communications*. Santa Monica, Calif.: Rand.

Burton, John. 1972. *World Society*. Cambridge: Cambridge University Press.

Castells, Manuel. 1996. *The Rise of the Network Society*. Vol. 1 of *The Information Age: Economy, Society, and Culture*. Oxford: Blackwell.

Cox, Robert. 1984. Social Forces, States, and World Order: Beyond International Relations Theory. In *Neorealism and Its Critics*, edited by Robert O. Keohane, 204–54. New York: Columbia University Press.

Deibert, Ronald J. 1997. Exorcismus Theoriae: Pragmatism, Metaphors, and the Return of the Medieval in IR Theory. *European Journal of International Relations* 3 (2):167–92.

------. 2000. International Plug N'Play: Citizen Activism, the Internet, and Global Public Policy. *International Studies Perspectives* 1:255–72.

------. 2001. Wars of the Wide-Area Networks. InfoTechWarPeace 9.11 Web site, <http://www.watsoninstitute.org/infopeace/911/deibert_wide.html> (accessed on 8 March 2002).

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press

------. 2002. Dark Guests and Great Firewalls: Chinese Internet Security Policy. *Journal of Social Issues* 58 (1):143–58.

Greif, Avner. 1994. Cultural Beliefs and the Organization of Society: A Historical and Theoretical Reflection on Collectivist and Individualist Societies. *Journal of Political Economy* 102 (5):912–50.

Hafner, Katie. 1996. *Where Wizards Stay Up Late*. New York: Simon and Schuster.

Huntington, Samuel. 1996. *The Clash of Civilizations and the Remaking of World Order*. New York: Simon and Schuster.

Keck, Margaret A., and Kathryn Sikkink. 1998. *Activists Beyond Borders: Advocacy Networks in International Politics.* Ithaca, N.Y.: Cornell University Press.

Krause, Keith, and Michael C. Williams, eds. 1997. *Critical Security Studies: Concepts and Cases*. Minneapolis: University of Minnesota Press.

Landa, Janet Tai. 1994. *Trust, Ethnicity, and Identity*. Ann Arbor: University of Michigan Press.

Legro, Jeffrey W., and Andrew Moravcsik. 1999. Is Anybody Still a Realist?” *International Security* 24 (2):5–55.

Lipnack, Jessica, and Jeffrey Stamps. 1986. *The Networking Book: People Connecting with People.* New York: Routledge and Kegan Paul.

Mann, Steve, James Fung, and Angela Garabet. 2001. Watching Them Watching Us: Self-Empowerment Through Wearable Computing Art(ifacts). Unpublished manuscript, University of Toronto.

Radcliffe-Brown, A. R. 1940. On Social Structure. *Journal of the Royal Anthropological Institute* 70:1–12.

Rorty, Richard. 1979. *Philosophy and the Mirror of Nature.* Princeton, N.J.: Princeton University Press.

Smith, Steve. 1999. The Increasing Insecurity of Security Studies: Conceptualizing Security in the Last Twenty Years. *Contemporary Security policy* 20 (3):72–101.

Stein, Janice Gross, Richard Stren, Joy Fitzgibbon, and Melissa MacLean. 2001. *Networks of Knowledge: Collaborative Innovations in International Learning.* Toronto: University of Toronto Press.

Thrift, Nigel. 1994. On the Social and Cultural Determinants of International Financial Centres: The Case of the City of London. In *Money, Power, and Space*, edited by Stuart Corbridge, Nigel Thrift, and Ron Martins, 327–55. Oxford: Blackwell.

Wellman, Barry, and S. D. Berkowitz, eds. 1988. *Social Structures: A Network Approach.* Cambridge: Cambridge University Press.

Yarbrough, Beth V., and Robert M. Yarbrough. 1999. Governance Structures, Insider Status, and Boundary Maintenance. *Journal of Biometrics* 1:289–310.

https://doi.org/10.1017/S7777777702000018 Published online by Cambridge University Press