Forthcoming Book

Low-Tech Threats in the Hi-Tech Age: Subversive Networks Across Ideologies, Technologies, and Times

by

Katya Drozdova, PhD

(2009)

Visiting Scholar, Stanford University, Hoover Institution on War, Revolution and Peace
Senior Research Scientist, National Security Innovations (NSI)
drozdova@hoover.stanford.edu
kdrozdova@natlsec.com

Synopsis

Adversaries use low-tech strategies to evade and attack US hi-tech defenses. Technologies change, yet covert organizing principles persist over time and across different organizations. Against overwhelming US technological and resource superiority, terrorists, insurgents, spies, and others continue to employ relatively rudimentary means – guided by ideologies reliant on subversive human networks – to conceal their operations and threaten US national and international security interests. Informed by history and current events, the book's systematic evaluation of technology's effects on subversive networks across different ideologies and times – from al Qaeda to KGB and others past and present – reveals a persistent and critical threat. The book explains this largely unrecognized and unaddressed low-tech threat phenomenon in and beyond the hi-tech information age.

A better understanding of this threat and its underlying principles will provide insights into threat detection and strategic implications as well as better counteraction approaches aimed at security as well as liberty protection. Employing information and organization theories, the study combines quantitative and discourse analysis methods using unique archival sources primary documents and other empirical data (including those available from the *"Boris Nikolaevsky"* and *"Fond 89" Collections* at the *Hoover Institution Library and Archives* at Stanford University as well as documents on current terrorist/subversive threats including materials from the US Department of Defense Harmony database available through *US Military Academy's Combating Terrorism Center* at West Point, among others). The book contributes to analytical perspectives and scholarly debates on these problems as well as their operational and policy solutions.

Abstract

Adversaries take advantage of low-tech means to target our open and increasingly hi-tech society. The technological gap is growing, but the nature of this asymmetric threat is not entirely new. Confronted by unmatched US technological and resource superiority, terrorist and other illicit organizations rely instead on relatively rudimentary means to conceal their networks and threaten US national and international security interests. These tactics challenge US government's detection and counteraction strategies built around "hi-tech" cyber-warfare components, including precision guided weaponry and electronic surveillance schemes. This "low-tech" challenge to hi-tech solutions relies fundamentally on human networks and allegiances. It uses civilian disguise combined with face-to-face and courier communications, cash or barter transactions, and basic-to-crude

weaponry (e.g., box cutters, homemade explosive devices, and suicide-bombers) to sustain terrorist operations. Such asymmetric tactics make these operations difficult to trace, prevent and counteract by hi-tech means. Whereas human intelligence approaches may be able to address such low-tech tactics, many constraints often necessitate alternative methods. Strategic use of ideologies, politics, information, and social pressure extend illicit networks' survivability by – among other things – curbing insider betrayals as well as outsider agent infiltrations.

Tracing technology's effects on such human networks reveal diverse threats' common core. For instance:

- Why have Osama bin Laden and Ayman Al-Zawahri been so difficult to find despite sophisticated US tracking technologies and 25 million dollar reward for information leading to their capture? – One obstacle is that they stopped using location-revealing satellite phones. Instead, the use of human couriers and tribal loyalties curbs information. They may have learned from earlier examples. A Soviet General turned Chechen separatist leader, Dzhokhar Dudayev, for instance, was located by intercepting his satellite-phone conversation and killed by sending laser-guided missiles to that spot. Such hi-tech traceability endangers terrorist survival. Low-tech, alternatively, offers them social protections that are quite difficult for Western governments to penetrate.
- Why are suicide-bombers widespread as a terrorist weapon? Technological jamming can disable remote bombs, but humans offer naturally guided weapons in disguise. The bomber's death also conceals his operational connections, allowing the network to survive. This is another aspect of the underlying low-tech threat. Understanding its common principles with those of covert communications, among other tactics, reveals subversive networks' strengths as well as vulnerabilities. Low-tech tactics, however, require insider allegiance.
- How to control dissent within subversive networks? A KGB defector, Alexander Litvinenko's, radioactive poisoning in London taught one lesson. Delivered by a cup of tea in public, this fatal attack mirrored Soviet tactics, such as a similar attempt on a defector KGB agent's life in 1957, as well as elaborate organizational and social controls structured around human surveillance, among others. The tactic also threatened public health and commerce revealing attack capabilities which, if delivered at random on a larger scale, could cripple a city if not a nation.

This book investigates the nature of such asymmetric and low-tech threats. It identifies their common principles and enduring impacts on national and international security affairs. It provides scholarly analysis with actionable insights. The analysis combines two complementary perspectives on an organization: an outside observer and inside participant views. From each perspective it examines how an organization's structure and processes involving technology-use relate to its mission and operating environment. Empirical data include observer records as well as participant narratives, primary sources and archives. Each perspective differs in what one can see and elucidate about an organization. Together they provide a fuller picture. Converging findings advance our understanding of the systemic nature of such low-tech threats. Results suggest counteraction approaches that take advantage of the US edge in hi-tech, yet build from the ground up to effectively target illicit adversary networks no matter what technology they use. Ability to better target our efforts in turns allows using less sweeping security measures aimed at security as well as privacy and liberty protections.

Book Chapters Outline

1. Main Idea and Approach

Subversive networks continue to threaten US national and global security. Examples include terrorist, insurgent, espionage, and illicit weapons proliferation networks. Specific organizations evolve over time but share common organizing principles. These include network organization structures and survival strategies based around largely "low-tech" technologies and tactics – taking advantage of direct human interactions as well as simpler, more self-reliant and infrastructure independent devices – that limit human network traceability, compartmentalize information, and conceal activity through legitimate social channels as well as covert ones. Though more advanced technologies tend to be more efficient in absolute terms, the lower-tech ones support the subversives' survival. Common constraints faced by organizations pursuing clandestine, illicit missions in hostile environments explain their technology strategies and other similarities. A better understanding of their common underlying principles provides insights into improved threat prevention and counteraction.

The book develops a new approach for understanding subversive organization failure modes and survival strategies. Such organizations' missions typically require them to prioritize security above efficiency considerations shaping vulnerabilities and strategies that are different from typical public or private organizations and can be traced through their mission-critical technology choices.

Technologies affect organizational abilities through networks that facilitate communications, actions and production. Organizations need networks not only to perform tasks but also to direct, coordinate, monitor and control actions. The technologies used in networks affect organization performance and survivability by enabling or restricting information flows, resource allocation, network connectivity, and action traceability. The technologies and network designs that organizations choose both enable and constrain them.

Specific technology choices diverge along a "hi-tech" vs. "lower-tech" dimension. Generally, low(er)-tech choices rely on interactions between people, whereas high-tech choices use the latest modern technologies to extend organization reach independent of people. Lower-tech solutions tend to be technologically simple, robust and rely on people and physical objects for limited transactions. Typically, they are not scalable to large networks, nor are their uses easily traceable. Hi-tech solutions extend organizational networks and knowledge bases, efficiently support multiple transactions, and their actions are traceable across networks. They are technologically complex and rely on costly infrastructures. As hi-tech frontiers advance, lower-tech options remain available to individuals and organizations.

Subversive networks take advantage of these options. The book defines and exposes the pervasive importance of low(er)-tech in our increasingly hi-tech age, as well as low-tech interplay with more advanced technologies and tactics exploited by security threats. Low-tech can be an asset (e.g., to terrorists for evading detection) or vulnerability (e.g., in cases where efficiency objectives dominate). Complex missions will require tradeoffs. How organizations make the tradeoffs can expose their strengths and vulnerabilities. Mismatch of technology to organizational network structure, mission and environment can be perilous – particularly in hostile environments. The book provides a quantitative model that uncovers broader principles, as well as specific case studies which illustrate how these principles emerge and manifest in action over time and across different organizations. The cases of al Qaeda and Soviet espionage networks (KGB) vividly illustrate these principles as well as their enduring implications for the study and practice of international security.

2. Conceptual Foundations: Combining Outside and Inside Perspectives on Organization

The book combines two complementary perspectives on organization: outside (observer) and inside (participant). The two views differ in what they can see and elucidate about an organization; approaches, criteria and types of findings will also differ. Combining them allows deeper and more comprehensive insights into organizations – how they work, fail, survive, and with what implications. This is critical for studying terrorist and other such secretive and dangerous organizations, information about which is limited and often tainted by intentional disinformation. The complementary perspectives compensate for one another's limitations supporting findings cross-validation. Combined results allow us to see what could not be seen before and better understand the threats and response options. Resulting insights contribute to scientific as well as practical objectives in defense, international politics, and homeland security areas.

3. Organizations from the Outside: Hi-Tech vs. Low-Tech Preferences and Case Selection

This chapter uses information theory and probabilistic information-entropy methods to identify missions and environments that implicitly predict contrasting organizational technology choices. It presents a model for quantitatively analyzing different organizations' observed technology preferences at the mission-critical level where their survival is at stake. To gain insight into preferences, we analyze relationships between observed technology uses and other attributes that reflect different aspects of organization missions, structures, resources, and environments. Results uncover regularities across a wide range of public, private and subversive organizations and generate observable dimensions along which organizations vary in terms of their technology preference for mission-critical activities. The Hi- versus Low-tech preferences are defined in context but in a way that allows specific, non-overlapping categorization and comparison. This analysis in prior research found that organizations which pursue non-monetary (e.g., ideological) missions in hostile environments consistently employ lower-tech technologies for mission-critical operations. Subversive networks fall into this category, from which we draw two specific illustrative cases – with different ideologies and environments but both characterized by an ideological mission and environment hostility, and both critical to the domain of international politics and security.

The cases are: al Qaeda and Soviet espionage networks (the book refers to the latter as 'KGB' recognizing that this is one of many names given over time to a complex of interrelated domestic and global networks comprising the Soviet state security apparatus – whose legacy still influences Russian politics, US security and world developments.)

4. Organizations from the Inside: Human Networks Design and Concealment Strategies

This chapter uses organization theory and case-study methods to analyze technology choices made by the two organization cases to implement their missions and conceal their operations. It applies discourse analysis methods to analyze text data derived from primary, archival, media, government and other records and sources documenting actual operations as well as organization participants' pronouncements and explanations of their work, motivations and worldviews. Text data are also quantified to examine activity and network patterns.

The case studies describe how technology links people to create alternative network organization designs. The cases illustrate how these designs emerge and generate fault-tolerant or fault-intolerant organizational outcomes in specific operations and contexts. To identify a design, the analysis traces how the technology

allows an organization to function and respond to risks, threats and new situations. Crises are especially informative as the use of technology during a crisis often reveals obscure or inactive organizational properties, turning points and adaptive abilities. Choices and outcomes depend not only on relations among network nodes, but also on network processes, participant skills, motivations, and overarching organizational narratives.

Based on organization theory and discourse analysis methodology, case study methods guide and integrate analysis across three levels – organizational 'deep structure' (mission, goals, ideology), surface structure (specific activity evidence over time), and manifestation structure (networks linking humans and technology in action and in context). Manifestation level also links findings across the deep and surface structures to generate a fuller picture of how and why human networks function, where they may be vulnerable, what sorts of faults or failures they face, and how they respond. Quantitative analysis based on technology use records elucidates specific network structures, properties and case comparisons.

4.1 Al Qaeda Case Study

Al Qaeda perpetrated the most devastating attacks on US mainland to date, targeting the very heart of our defense and financial engines, the Pentagon and the World Trade Center. This was achieved without sophisticated weaponry, but using covert human networks and technologies as simple as box-cutters as well as the knowledge of our own civilian infrastructures and how to turn them against us. How does al Qaeda manage this and many other attacks? The case study uses specific operation examples to trace out al Qaeda organizing principles, where they are strong, and how to detect and destroy them.

Data sources include documents and al Qaeda archives captured by the US and Coalition forces in Afghanistan, Iraq and elsewhere (e.g., available from the US Department of Defense *Harmony Database* including documents accessible through the United States Military Academy's Center for Counterterrorism Studies at West Point and other sources). Other sources include US legal proceedings from terrorist trials, unclassified or declassified intelligence reports and other government documents, al Qaeda leadership and member statements, and various media records. The sources are triangulated and assessed for accuracy, veracity and other relevant attributes.

The analysis draws on several specific operations as well as systemic patterns and context to extrapolate beyond the specifics. Specific operation examples include the 1998 bombing of US Embassies in Kenya and Tanzania – a plot that has not only inspired and laid foundations for many other attacks, but also one that reveals al Qaeda vulnerabilities. There, a suicide bomber survived and was captured. He provided in-depth insights into the inner workings of al Qaeda. By triangulating evidence from this operation with others, such as 9/11 and more recent developments, the case study identifies and explains the al Qaeda organizing system that continues to manifest in current situations and is likely to survive – unless specifically defeated at its low-tech level – as, at the core, it is based on age-old, low-tech, tried and tested means designed to asymmetrically evade and survive many typical US offenses.

4.2 'KGB' Case Study

The Soviet Union was notorious for using terror against its own people as well as supporting communist insurgencies and violent groups around the world. State security networks played a key role in protecting the state from its own citizens as well as orchestrating worldwide operations. The study of

al Qaeda and related current terrorist organizations also revealed similarities to Soviet operational methods particularly for covert organization, human networks concealment, disinformation, and diversion tactics. Thus there are at least analytical links between the two cases, as well as possible knowledge transfers and network links that the in-depth study will bring to light. A deeper study of KGB networks offers not only its own insights into the principles of covert networks but also into similarly structured current and potential future security threats.

The case study uses and brings to light unique historical accounts assembled by the Russian historian Boris I. Nicolaevsky and safeguarded in the Hoover Institution Archives' *Nicolaevsky Collection* covering the Soviet security apparatus. Much is known about Soviet covert networks from their victims. But the Nicolaevsky Collection offers rare insights into how this system worked and where it failed from the 'insider' viewpoints of its perpetrators – including personal accounts of their work by military and foreign intelligence and counterintelligence agents as well as domestic security agents. Other data sources include media and government reports as well as *Fond 89 Collection* also at the Hoover Institution Archives covering the Soviet communist party and state apparatus. These documents provide unprecedented views into the inside operations of KGB and related entities from the little publicly known perspectives.

The analysis again draws on several specific operations as well as systemic patterns and context to extrapolate beyond the specifics. Specific operation examples include attempted radioactive poisoning on a defector KGB agent Khokhlov in 1957, which mirrors some of the circumstances surrounding the 2007 Litvinenko case, as well as Soviet networks active in Iran and elsewhere in the Middle East shaping US security concerns, which still reverberate today.

5. Integrated Findings: Toward a theory of Fault-Intolerant Network Organization (FINO)

Integrated findings combine insights from the outside and inside perspectives into a common theoretical framework. The framework builds upon and extends the author's dissertation work on fault-tolerant and fault-intolerant network organizations. These network organization classes differ systematically in terms of their human network design, vulnerabilities and technology use implications. FINOs tend to be particularly vulnerable as well as dangerous – including the two cases and other subversive organizations. This novel perspective offers new lessons-learned from history and across different organization types – by comparison and contrast. It enables better understanding and estimation of secretive organization properties from their observable traits and technology-use patterns.

6. Policy and Operational Implications

The cases and their underlying principles found here still play out in world politics and will likely continue to shape international affairs and homeland security concerns. Al Qaeda continues to present one of the major US national security threats, and Russian government, with a KGB man at the helm, has demonstrated a cooler if not confrontational course with the West. The principles identified and explained by the book also play out in other organizations and potential threats. This book's analytical approach and findings provide a novel unifying view on a variety of threats. It aims not only to contribute to scholarship in analytical perspectives on politics, but also to assist policy makers and national security professionals in better understanding and addressing key defense and challenges. The work also aims to be useful to a new Presidential Administration as it works to assess and addresses many security and policy challenges anew.

7. Conclusion

Conclusion summarizes key findings, research approach innovations, and practical applications.

Appendix

Appendix provides the mutual information entropy model details and data summary.

About the Author

Ekaterina (Katya) Drozdova, PhD, is a Senior Research Scientist at National Security Innovations (NSI) and Visiting Scholar at Stanford University's Hoover Institution on War, Revolution and Peace. Dr. Drozdova's work focuses on the role of technology and network organizations in US National and international security issues, with emphasis on asymmetric threats in the post-9/11 environment. This includes problems of countering terrorism, insurgency, and weapons of mass destruction proliferation; advancing cyber- and energy security; and strengthening both security as well as liberty. As part of NSI, Dr. Drozdova conducts scientific research and provides findings, analytic models, technology, strategy and policy analyses and insights for the US Department of Defense (DoD) as well as Intelligence and Diplomatic communities' professionals, including work on DoD's cross-agency Strategic Multilayer Assessment program, among others.

Dr. Drozdova has published articles on issues ranging from detecting and estimating terrorist networks to understanding Cold War legacy in modern global developments, among others. She also contributed chapters to published books on the transnational dimension of cyber crime and terrorism and on unconventional warfare issues. She has served as a member of DoD's Command and Control Research Program (CCRP), Research Scholar at the Alexander Hamilton Center, Politics Department, New York University (NYU), as well as Science Fellow and MacArthur Affiliate at the Center for International Security and Cooperation (CISAC) at Stanford University. She was also researcher with the NSA-funded Consortium for Research on Information Security and Policy at Stanford University. Dr. Drozdova earned her Ph.D. in Information Systems from NYU's Stern School of Business, Department of Information, Operations, and Management Sciences. The main focus of her dissertation is the impact of technology choices on organizational fault-tolerance in hostile and competitive environments, with emphasis on the questions of how and why organizations use technology to counter or cloak their human network vulnerabilities. Her Bachelor's degree in International Relations and Master's degree in International Policy Studies are from Stanford University.