Effects of Adversarial Interaction on the Adoption and Adaptation of Disruptive Communications Technologies

A Brief Overview

SETH LEWIS, TERRY STUDER, MARTIN VOSHELL

Mitigating the effects of disruptive communications technologies is quite challenging given how intelligent adversaries with dynamic organizational structures constantly adopt and adapt. This is further complicated by the rapid evolution of modern communication such as the World Wide Web. The current work proposes a descriptive model of adversarial interaction in order to support analysts and decision makers in anticipatory and adaptive collection to help avoid strategic and adversarial surprise.

INTRODUCTION

Traditional models of technology adaptation and adoption often ignore two main issues when they focus on disruptive technologies.

1) **Varying organizational structures** - Some groups are organized according to a highly compartmentalized, dynamic, and cellular structure, whereas other groups operate in a traditional, hierarchical manner.

2) **Effects of an intelligent adversary** on the technology adoption and adaptation cycle - In highly technical societies, technology will benefit the attacker, at least initially. The enemy rarely innovates for innovation's sake; most often they are forced to adopt or adapt to pressures put on them by their adversary. This adversarial relationship compounds the risk factors that groups must consider when adopting or adapting a new technology use.

Adversarial groups use both indirect and direct communications, depending on their goals, stance, capabilities, and doctrine. This manifests in how they share information and plan operations through:

- **Indirect Communication** – Groups knowingly distribute information to a mass audience but retain limited control as to who reads or listens (e.g. blogs, websites, message boards)

- **Direct** – Groups communicate with a specific intended recipient (e.g. cell phones, e-mail draft correspondence, instant messaging)

A CURRENT PERSPECTIVE

The figure below, developed by the RAND Corporation, illustrates one view of how terrorist groups conduct operations. In the operational
planning and execution phase of their activities, there is more reliance on direct communication, whereas throughout the recruitment, indoctrination, training, and propaganda phases reliance shifts to indirect forms of communication. To accomplish their objectives in this phase terrorists must disseminate information to a mass audience. If they cannot reach an adequately large audience then the use of that particular technology is insufficient.

What the model below fails to describe are the complex communicative interactions that are taking place at different stages of the terrorists’ activities.

**TOWARD DEVELOPING A NEW MODEL**

The cycle below serves as a model based on adversarial interaction to describe the adoption and adaptation of disruptive communications technologies by enemy groups. The speed of the cycle varies depending on whether the communications usage method in question is direct or indirect. The cycle revolves around a set of core communications procedures that constantly supplement technical communications. A cycle dealing with direct communications moves more quickly. Information transmitted using this method would be actionable for an adversary and also present the greatest risk of interception for the group. A group that adopts blogs as a technology, for example, will maintain its use as long as it fits into a set of criteria that dictates its effectiveness. If the situation changes, or is perceived to have changed due to an enemy’s actions, then the group will be forced to innovate or adapt a new communications usage technique or risk being exposed.

In short:

- Adversaries will only adopt a new usage technique if their enemy forces them to through developments of a counter-measure. For example, reports suggest al-Qaeda uses e-mail to correspond and aid in operational planning. Upon realizing that transmitting e-mail is vulnerable to interception, they may alter their usage.

- Adopting a new usage technique allows them to accomplish their goals as dictated by usage criteria. There is evidence al-Qaeda transitioned to using drafts of e-mails as a type of “electronic dead drop.” This adoption enables multiple cell members to send
and receive direct communications while retaining their anonymity and remaining less vulnerable to electronic interception.³

Use of weblogs by Jihadist terrorist groups is another good example of how this cycle works. As seen in Appendix A, terrorists make use of many of the same technologies as any other group and have evolved their usage in line with much of the general public. The use of weblogs is one example of this usage. Jihadist groups use weblogs for indirect communications to accomplish their goals of recruiting new members, indoctrination, and even training group members. By its nature indirect communications is meant to reach a large audience and has very little control over who can access the information. The communications to a point is protected by some characteristics of the Internet itself. An analyst trying to sort through all of this information has a difficult time with data overload, trying to determine what information is legitimate and what is not, and trying to keep up with new sites being put up continuously.

A counter-measure to handle some of these problems is being developed by the University of Arizona. This counter-measure, called Dark Web, is an open source data-mining tool capable of capturing and sorting through all terrorist blogs on the Internet. In theory, all of this can result in a reduction of the amount of “noise” and give the analyst less, more important information to deal with. These blogs no longer would be secure as a byproduct of analyst data overload. In effect, some of the terrorist groups’ recruitment and training sources and methods might become compromised, thereby making the use of blogs too risky. Because all intelligent adversaries are constantly monitoring to see if their

communications have been compromised, eventually the Jihadist groups will become aware of that this communications method is insecure be forced to adapt their usage. Here pressure from the adversary is what changes the situation forcing adoption.

A possible forced adaptation in response to Dark Web could be for terrorists to begin using coded messages, communiqués hidden in neutral sounding text, or more technical methods such as steganography, which conceals messages in plain sight within digital files (e.g. music and photos). The terrorists’ use of steganography would serve as an adaptation by allowing them to circumvent the Dark Web program’s text-based focus and capabilities. Evidence points to steganography becoming increasingly vital to adversarial communication efforts. In October 2001, French intelligence officials disrupted an al-Qaeda affiliated plot to blow up the U.S. Embassy in Paris. An investigation revealed that the perpetrators employed steganography in their planning phases. However, this would likely be a temporary adaptation. As mentioned above, steganography is most effective in a direct communications role. So, while this meets some of their requirements, to have secure communications, it does not fill the gap in their indirect communications efforts. If they began using non-technical forms of steganography then they would be falling back on the core communications functions seen in the center of the cycle.

While the adversary always is forcing their counterpart to adapt and adopt new communications usage techniques they are not always successful. A historical example of some adversarial groups that either successfully adapted their communications methods and survived and others who did not adapt were the Soviet Army and the Afghan Mujihedeen fighters during the Soviet-Afghan War. The Soviet Army knew that their radio communications had been compromised by the guerrillas and that not only were they able to avoid attacks from the Soviets they were able to target Soviet units and disrupt their operations using disinformation, but they chose not to adapt their methods. Some of the Afghan units on the other hand also used radio communications and it was monitored by the Soviets, but they chose to adapt to this by breaking squelch on the radio to signal to other units instead of using the radios for voice communications. This issue, among many others, eventually contributed to the Soviet Army’s ultimate defeat and withdrawal from Afghanistan.

**IMPLICATIONS AND PAYOFF FOR FUTURE SYSTEMS**

A critical component often ignored when conducting research in information analysis is the dynamic interaction of an intelligent and adaptive adversary. The uncertainty created by these interactions produces the classic fog and friction of war between opponents.

The modern ‘open source’ enemy can be well funded, can be quite risk tolerant, and can utilize technology as a force multiplier to carry out their goals. In the model we argue that the fundamental patterns of collaborative work are the same, however the changing nature of technology can drastically impact and facilitate defensive and offensive activities.

All technology is dual-use. The dual-use transfer of technology and innovation is tighter than ever before and the lines between military and civilian use are blurred. Dual-use technologies used to be rare, but today information technology transfer and consumption is rapid and we constantly see applications and adaptations of technology in unanticipated uses.

---

4 Kolata


6 Kolata
Forms of attack and defense are the same across military and civilian sectors—from routers, switches, and servers to protocols, and applications. This creates new and emerging gaps for malicious adversaries to leverage and exploit.

"Technology creates security imbalances."—Schneier, 2007. Disruptive Technology and Innovation can be defined as an unanticipated use of a current technology by an adversary in order to more effectively accomplish their objective(s). As attack tools become more plentiful, powerful, and easier to use, adversaries are quick to adopt and make use of technology that lets them accomplish their goals with less effort.

With recent IT advances, technology plays a major role in the mediation of operations, it amplifies capabilities and vulnerabilities in a one:many fashion, technological skill is separated from ability, and actions can be carried out at a distance.

**Appendix A**
The chart below is a good illustration of how public technology adoption has progressed over time. This has resulted in increased connectivity between people and the rate of connectivity has dramatically increased after the advent of the Internet. Today, it is much easier to collaborate and network with other people, using tools like Wikipedia, Myspace, and Facebook. Terrorist groups use the same technology as the public to stay connected and share information. The difference is that the rates of adoption and what is actually adopted are different due to the impact on these groups from their adversaries.

Adapted from The New York Times “Consumption Spreads Faster”