

# INTERNET-DERIVED TARGETING: TRENDS AND TECHNOLOGY FORECASTING

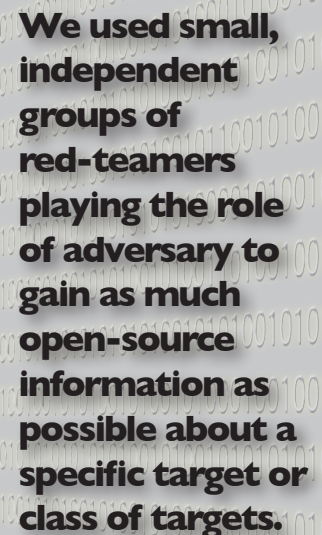
Jason A. Dechant and Zachary S. Rabold

## The Problem

For several years, mounting evidence has pointed to adversary use of the Internet as a resource for target selection and attack planning. One recent example was a bomb plot targeting former President George W. Bush's residence; the suspect's computer revealed extensive use of the Internet for targeting purposes.

To better anticipate nefarious use of the Internet and understand how it may be used for targeting purposes, the DoD developed an experimental red-teaming approach involving multiple independent teams emulating adversary targeting and planning cells. The teams are given laptop computers, uninterrupted workspace, a wireless Internet connection, and three days to complete their mission. The purpose of these experiments is to determine whether the Internet may be used to develop a list of potential targets to attack, to focus the list based upon a set of criteria, and to design notional concepts of operations for attacking targets.

Between 2008 and 2010, IDA conducted 10 Internet-Derived Targeting (IDT) missions. For each of these missions, we used small, independent groups of red-teamers playing the role of an adversary to gain as much open-source information as possible about a specific target or class of targets. At the conclusion of the tenth IDT mission, DoD asked IDA to conduct an analysis of all of the missions to assess what could be learned about using the Internet for targeting. Additionally, we were asked to consider how adversary use of the Internet may evolve in the near-term (between 2010 and 2015), considering the proliferation of and advances in online technologies. Specifically, DoD asked IDA to examine how evolutions in the capabilities of mobile online technology, social network platforms, and online imagery may have implications for adversary targeting activities.<sup>1</sup>



**We used small, independent groups of red-teamers playing the role of adversary to gain as much open-source information as possible about a specific target or class of targets.**

<sup>1</sup> IDA also reviewed how online search functions and “enthusiast” websites – websites that provide valuable targeting information from communities of amateur followers – will evolve to support online targeting in the next five years. These online features are discussed in detail in Chapter 3 of Jason Dechant and Zachary Rabold et. al. *Internet Derived Targeting: Trends Analysis and Technology Forecasting* Paper P-4687 (Alexandria, VA: Institute for Defense Analyses, 2011).

## IDT Trends Analysis

IDA researchers compiled lists of websites used during the 10 missions. Using automated software,<sup>2</sup> from the aggregated list of websites, natural categories emerged. We determined which individual websites were most frequently used across all IDT missions, for each IDT individually, and for different classes of targets. A number of findings emerged from the analysis of the 10 missions:

1. Commercial websites (e.g., those of private companies) were the most frequently used category of websites shown in Figure 1.
2. The majority of the most useful websites across all IDT missions were from government and defense domains, though common news media sites also proved useful.
3. Despite the proliferation and increased use of social networking sites (e.g., Facebook), blogs and message boards, those sites were not used frequently.

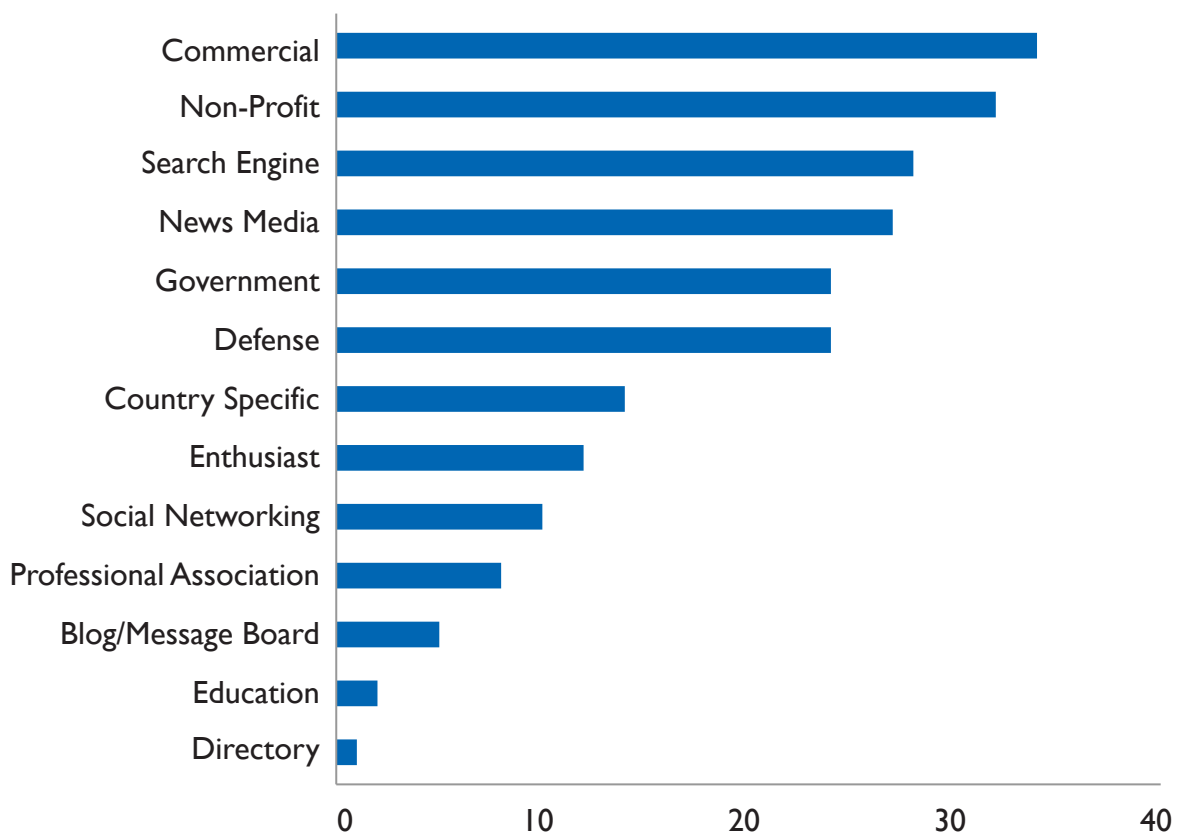


Figure 1. Most used categories of websites during IDT “red-team” missions, 2008-2010.

<sup>2</sup> An IDT red-team member’s “online signature” is a traceable, digital path used by that member to select specific mission-related targets. Red teamers’ signatures are collected by using a computer tracking program (SpectorPro), online search history, and other online track methods, as well as a conscious effort by red teamers to record their specific online behaviors.

---

## Technology Forecasting

The second part of the study examined how adversary use of the Internet may evolve in the near-term (2010-2015) given the proliferation of and advances in online technologies. This began with an in-depth literature review of key technology areas that may assist and enable adversary targeting using the Internet: (1) mobile online technology, (2) social network platforms, and (3) online imagery. To supplement the findings of the literature review, the project team interviewed experts in each technology area's industry, as well as relevant professionals at IDA. These interviews, if not conducted in a one-on-one setting, took place at official on-the-record industry meetings, seminars, and workshops - mainly at the Web 2.0 Expo held in New York City from September 27-30, 2010 - or in exchanges by telephone and e-mail. The three technology areas where advances are expected in the near-term are discussed below.

### *1. Mobile Online Technology*

In the near-term, mobile near real-time, online technology will enable adversaries to obtain more than a basic understanding of targets using mobile augmented reality and improved Internet browsing capabilities.<sup>3</sup> Additionally, static imagery capabilities (e.g., Google Earth) combined with mobile, Internet-connected imagery (e.g., camera phones and online webcams) will allow adversaries to project themselves onto a common mapping plane with a

target and conduct "omnipresent" real-time (or near real-time) surveillance of a target. From a human targeting perspective, this near real-time surveillance can be done electronically and instantaneously with little or no person-to-person interaction with the target.

### *2. Social Network Platforms*

Trends in social networks facilitate the information collection and information consumption stages of targeting. In its examination of social network platforms, IDA found that five developments will drive the growth and utility of social networks for targeting purposes: the integration of facial recognition technology, content integration across websites and platforms, geo-location awareness, cross-platform integration, and user-generated applications. The implications of these developments to social networks center on their increasing importance in everyday social interaction and the increasing amounts of data they connect and replicate. While personal information on a target may be more useful than it was in the past, the volume of data available also means there is more noise to filter out.

Social network information can be exploited in a variety of ways. For example, it is possible to map clusters where social network use was important and unimpeded and, by contrast, locations where it was discouraged. Done in the proper location, it is possible to locate where sensitive work may be taking place

---

<sup>3</sup> Augmented reality on mobile technology uses a device's cameras, compass, GPS systems, and data browsing and storage capacities to allow users to get information about a location or facility and overlay the information on a common mapping plane.

---

that would warrant more extensive restrictions on mobile and Internet use. In addition, accessing a single networking site will allow an adversary to target the exposed individual's connections by seeing his or her social, economic, and lifestyle preferences. There is also the opportunity to use social networks for denial and disruption attacks, or as part of information operation (IO) efforts.

Social network use will continue to expand globally, especially in currently under-connected and under-utilized locations. As developers and advertisers seek ways to exploit real-time content, social networks are facilitating a convergence of previously compartmentalized content and activity, resulting in an increased aggregation of content in one fixed place with recognized vulnerabilities. Personal data are becoming more easily accessible via social plug-ins in cross-platform applications (e.g., connecting Facebook and Twitter accounts). Increasingly, gaining access to a single networking site will open up an individual's entire social networking universe to exploitation.

### *3. Online Imagery*

As commercially available satellite technology enables higher resolution imagery and more frequent refresh rates, it will become increasingly easy for adversaries to use open-source platforms to geo-locate and geo-orient locations of interest and to determine best approaches. Based on recent developments in online, open-source imagery, it appears there is a strong demand for real-time functionality among users of online imagery platforms. It does not appear as though real-time satellite

imagery will be accessible in the near-term; however, it does appear that there will be increased near real-time functionality across online imagery platforms which could provide targeters with useful information about a given location.

Augmenting online satellite imagery with user photographs, webcams, tracks, and near real-time layers will provide opportunities for adversaries to garner previously unforeseen insights about a location. Additionally, growing online imagery capabilities allow targeters to detect change in near real-time, over long periods of time, and in a time series. Adversaries casing targets can notice changes in a target's security posture and perhaps even defenders' response times and routes of approach. Targeters may also be able to supplement and, potentially, even replace harbor sites by using emerging online imagery capabilities in combination with tracking technologies and applications. Used in combination, changes may be observed over long periods of time or constantly, as opposed to the finite timeframes available during ground reconnaissance missions.

## **Implications for Targeting Activities and Defense Intelligence**

IDA's technology forecasting analysis revealed not only noteworthy emerging firms, technologies, and capabilities, but also several trends relating to how individuals, groups and societies are leveraging elements of the Internet.

---

The technology areas researched by IDA do not change targeting fundamentals. The opportunities and risks associated with the planning phases of a targeting operation are instead redistributed.

While the quantity and quality of information yielded from remote reconnaissance would appear to be greatly improved using expanded Internet capabilities, targeters still risk exposure. As adversaries utilize advanced Internet capabilities, they expose themselves to the same identification vulnerabilities as their targets, creating opportunities for offensive targeting.

Successful targeting still requires key pieces of information, not all of which may be available on Internet sites. Thus, denial and deception activities will likely continue to be worthwhile.

The proliferation of sensors on vulnerable platforms, coupled with

their increased use, enables individuals to act as sensors and be used in many different ways. This research points up the importance of being attentive to the potential for targeters to leverage such witting and unwitting intelligence sources and assets.

The results of these IDA analyses have been used by government sponsors to better understand adversary use of the Internet and to expose potential vulnerabilities posed by open sources.

---

*Jason Dechant is a research staff member in IDA's Strategy, Forces and Resources Division. He is currently a doctoral candidate at George Mason University's School of Public Policy.*

*Zachary Rabold is a research associate in IDA's Strategy, Forces and Resources Division. He holds a master's degree in international relations from the University of Chicago.*