acmqueue National Internet Defense— Small States on the Skirmish Line

Attacks in Estonia and Georgia highlight key vulnerabilities in national Internet infrastructure.

Ross Stapleton-Gray and Bill Woodcock, Packet Clearing House

Despite the global and borderless nature of the Internet's underlying protocols and driving philosophy, there are significant ways in which it remains substantively territorial. Nations have policies and laws that govern and attempt to defend "their Internet"—the portions of the global network that they deem to most directly impact their commerce, their citizens' communication, and their national means to project social, political, and commercial activity and influence. This is far less palpable than a nation's physical territory or even than "its air" or "its water"—one could, for example, establish by treaty how much pollution Mexican and American factories might contribute to the atmosphere along their shared border, and establish metrics and targets fairly objectively. Cyberspace is still a much wilder frontier, hard to define and measure. Where its effects are noted and measurable, all too often they are hard to attribute to responsible parties.

Nonetheless, nation states are taking steps to defend that space, and some have allegedly taken steps to attack that of others. Two events in the recent past illustrate the potential vulnerabilities faced by small nation states and suggest steps that others may wish to take to mitigate those vulnerabilities and establish a more robust and defensible Internet presence. The first was an attack on Estonian Internet infrastructure and Web sites in May and June 2007. The second was a cyber attack against the Georgian infrastructure that accompanied the Russian incursion into South Ossetia in August 2008.

ESTONIA

Tensions had been building in Estonia in the spring of 2007 over the country's plans to relocate the Bronze Soldier, a Soviet war memorial, and the capital, Tallinn, experienced several nights of rioting. The subsequent cyber attacks are believed to be a consequence of the memorial's relocation.

An attack on Estonian Internet infrastructure and Web sites began at 11 p.m. local time, midnight Moscow time, Tuesday, May 8. The attack was effectively mitigated by 7 a.m. the following day but continued to be visible in traffic logs for exactly 30 days thereafter. That time period, together with the fact that the attacking botnets' signature was identical to that used in prior Russian Business Network spam-sending campaigns, suggests that this was a one-month attack for hire (or was intended to look like one). Unfortunately, such attacks, either threatened or launched for commercial extortion, have become commonplace. Based on offers visible on the black market at the time, the attack likely cost between \$200 and \$2,000 to hire. Like many politically motivated attacks, it combined a DDoS (distributed denial-of-service) attack against Internet infrastructure with DDoS and attempted defacement attacks against the Web sites of Estonian banks, media outlets, and government.

The Estonian defense was notably successful, and there are a number of lessons to be taken from it by other countries wishing to avoid a cyberwarfare defeat. The simplest summary of the dynamics

of a DDoS-based cyber attack is as a numbers game. An attacker with greater network capacity than the defender will be able to overwhelm the defender's network, while retaining sufficient capacity to support its own needs at the same time. Such an attack would be deemed successful. An attacker with less bandwidth than the defender would exhaust itself in consuming the defender's capacity, while the defender might well retain enough excess capacity that its population would not be significantly inconvenienced; such an attack would be considered unsuccessful.

Viewed in closer detail, there are different kinds of network capacity and different mechanisms for improving and defending each. They can be placed in four categories: local or internal capacity; external connectivity; name resolution capability; and defensive coordination.

LOCAL CAPACITY

Local capacity or bandwidth is most familiar as one's initial connection to the Internet. This local loop, or last mile, is the copper wire or fiber line in the ground or on poles, or the wireless link, that carries signals from the customer to an ISP (Internet service provider). A robust local-loop infrastructure consists of buried fiber-optic cable interconnecting each business or residence with multiple ISPs over different physical paths. Ideally, these service providers ought to be in competition so they cannot be collectively suborned or sabotaged, and so their prices are low enough that people can actually choose fluidly among them. A sparsely supplied market for local connectivity can create bottlenecks and make attractive targets. In Estonia's case, multiple independent fiber infrastructure operators existed, and many different ISPs built a healthy, competitive marketplace on top of that. More—and more diverse—domestic fiber is always better, but Estonia's was more than sufficient.

EXTERNAL CONNECTIVITY

More important to defensibility is the ecosystem for the providers' own connectivity within that domestic context. The modern means to create an effective mesh of providers is via Internet exchange points, commonly abbreviated IXP. The world has about 330 IXPs at the moment, and that number has been steadily increasing. Each IXP has a specific physical location and connects a community of ISPs that meet as peers at the exchange. Some countries, such as the United States, have many IXPs. Others, such as the Netherlands and Germany, have very large IXPs. Many smaller countries have exactly one exchange, located in the capital city. But the greatest number of countries, typically the smallest ones, have no IXP at all. This means that they are heavily dependent for their *domestic* connectivity upon *international* data circuits. Imagine a situation in which there were no local telephone calls, only calls overseas; to reach someone next door, you would have to make a call that went overseas *and then back again*, at twice the cost.

This is the situation in most less-developed countries, as a result of misunderstanding Internet economics and topology. Countries in this situation are extremely vulnerable to having those external lines of communications cut or overburdened, since that causes not only international but also domestic communications to fail, and thus the ability to coordinate a defense fails as well. A strong domestic Internet exchange point is the first and most critical component of a cyberwarfare defense. A redundant pair of IXPs, or one in each major city, is the desirable goal. A redundant pair of IXPs in Tallinn formed the linchpin of the Estonian defense.

International communications capability is necessary for conducting business in a global economy. It's also needed for defensive coordination with outside allies in order to protect a nation's

international capacity. International capacity is the asset most easily targeted from the outside, and it is perhaps the most challenging to defend from the perspective of the state, since it's a multinational private-sector resource. In most countries, each circuit that crosses the border is controlled by one company at one end, another company at the other end, and a third in between. In turn, many of these companies are themselves consortia of other multinational companies. On the domestic end of a circuit regulatory jurisdiction is generally clear, though limited and perhaps difficult to enforce; but on the other end it is nearly impossible even to influence. Diversity is thus key to optimizing the survivability of international connectivity.

Estonia had numerous privately controlled data circuits crossing its borders, with the other ends located in several different countries. Of these, the most significant were large Scandinavian and Western European ISPs with which Estonian ISPs had commercial relationships and that were based in diplomatically friendly neighboring countries. This is an optimal situation, and when push came to shove, Estonia received fast and effective aid from the ISPs at the other ends of those circuits.

NAME RESOLUTION

The ability to resolve domain names domestically is another critical infrastructure capability. The DNS (Domain Name System) is the Internet's directory service, providing Internet-connected computers with the ability to map the human-readable domain names in e-mail and Web addresses to the machine-readable binary IP addresses used to route traffic within the network. Domain names are resolved to IP addresses (and vice versa) by iterating through a delegation hierarchy of DNS directory servers, starting at the "root" and progressing through TLD (top-level domain) name servers such as .com and .net, to the organization-specific name servers that hold the particular answer one is looking for.

If connectivity is broken between users and any one of the name servers in the delegation chain from the root down to the specific one they're looking for, then the users will be unable to resolve the domain name they're looking for, and unable to reach the corresponding Web site or send the e-mail, regardless of whether they have connectivity to the Web site or e-mail addressee. If the directory service is broken, you can't *find* things, even if you could, hypothetically, *reach* them. Estonia did not have any root servers within the country at the time of the attack, and still does not today. This is one of the few weak points of the Estonian defense and would have become more debilitating over the course of an attack that had been more effective for a longer period of time.

DEFENSIVE COORDINATION

The final component of an effective cyberwarfare defense is coordination. Knowing that one is under attack is an intelligence function. Identifying and characterizing the attack is a forensic analytical function. Communicating this information to the ISPs that can mitigate the attack is a communications function. These functions are most often coordinated by a CERT (computer emergency response team), sometimes called a CIRT (computer incident response team). A CERT is the glue that holds a defense together, providing expertise, analytical facilities, and open lines of communication between the many organizations that are party to the defense or have some stake in its success.

CERTs provide training and preparedness workshops, maintain and exercise contact lists, and observe trends and find patterns in online criminal, military, and espionage activity. When

a country is under attack, CERTs help individual organizations identify which portions of the attack are directed against them particularly, as opposed to those that they're feeling the effects of incidentally. CERTs provide the expertise to help those organizations with the very specialized tasks of discerning attack traffic from legitimate traffic and developing filters that will block the attack while protecting their ability to conduct business. CERTs will then communicate those filters up the path of ISPs toward the attackers, blocking the malicious traffic at each step, pushing the boundary of the cleaned network away from the victims and toward the attackers.

GEORGIA

A little more than a year after the Estonian incident, Georgia was subjected to cyber attacks in conjunction with the Russian incursion into South Ossetia in August 2008. This more complex attack combined Georgian targets with domestic media outlets that were perceived to be reporting news from a Georgian perspective.

Much of what had worked well in the case of Estonia did not in the Georgia attack. Relative to Estonia, Georgia suffered from two crippling deficiencies: Georgian international connectivity was far more limited, hence more vulnerable. Most of its international links were through Russian territory; and unlike Estonia, Georgia had no IXPs. As with Estonia, Georgia lacked a DNS root server, but that was mooted by its limited infrastructure being easily overwhelmed.

Given the relatively modest infrastructure and comparative lack of e-commerce to be affected (and all dwarfed in significance by an actual shooting war), it may be more difficult to extract lessons from Georgia's experience than from Estonia's. One noteworthy issue in the case of Georgia, however, was the number of offers made by governments and corporations to "mirror" Georgian Web content. If the Georgian government desired to reach a non-Georgian audience for sympathy and support, then distributing that message to parties outside Georgia and in regions of the Internet far less amenable to denial-of-service attacks would be a worthwhile strategy.

WHY "CYBERWAR?"

The mere fact that significant conversation is still occurring more than three years after the attacks on Estonia indicates that even if the destructive impact was minimal, the overall information warfare effect was significant. The return on a very small investment was disproportionately high; these margins suggest that cyberwarfare techniques will continue to be applied until they become considerably more expensive or less noticed.

It's worth understanding what was successful about the attack and what was successful about the defense. Viewed in the large, the Chinese cyberwarfare doctrine upon which the attacks were patterned states that one of the principal goals of an attack is to dispirit an adversary's civilian population, reduce their productivity, and cause them to withdraw economic, and eventually moral, support from their country's engagement in the conflict. This was not the SCADA attack—an attack on the cyber aspects of physical systems, with the intent to cripple the latter—that is so often warned of in the United States. (SCADA, for supervisory control and data acquisition, is a catchall label for the various systems used to manage industrial systems and processes, from factories to pipelines to transportation networks.) Rather, the Estonia incident was a pure information-warfare attack, attempting to convince Estonians that the information-economy infrastructure of which they were so proud was vulnerable and unsound, that their work in that sector was of little value,

that their adversary was more capable and better prepared, and that in a more pitched conflict, their defeat would be inevitable. A population that would take such a message to heart would indeed be unwilling to support conflict against the attacker.

The Estonia attack had very little success in concrete terms, and little more success in information-warfare terms, relative to the Estonians against whom it was directed. Because of its apparent state-on-state nature, and Estonia's status at the time as the most recently admitted NATO ally, the attack managed to garner a surprising degree of attention elsewhere, though. The attacks against Georgia were far more effective, but Georgia did not have as far to fall and the conflict on the Internet paled in comparison to the actual shooting war in its territory. One might accurately term both the Estonia and Georgia cyber assaults as skirmishing; the attack on Estonia amounted to little more than a nuisance, in part because of its scale and in part because of the effectiveness of the response.

Without a doubt, any major shooting war would see complementary attacks against the adversaries' information infrastructure, including their national presence on the Internet—suppression of the means to coordinate and organize has long been a basic tenet of warfare. It's perhaps early to assess the impact of cyberwar, absent "real war"; the attack against Estonia was too slight to measure significant effects, while the attack on Georgia was just a sideshow to a widely, physically destructive conflict.

The ultimate source of both attacks remains murky. Many assertions have been made, but there has been little actual discussion of the question of state involvement in cyber attacks. Plausible deniability has become the watchword in cyberwarfare, and accordingly, attribution has become a major focus of effort, consuming far more resources than does actual defense.

DEFENDING THE SMALL NATION STATE

Ensuring the Internet security of a small nation state entails investment in four areas: ensuring physical network robustness; securing the interconnection of participating networks through exchange points; securing the data and services required to keep the Internet running; and developing an effective response community.

In advance of any threat, a nation should take steps to ensure that its networks are connected to the rest of the world via diverse international transit links to different unrelated transit providers in different, unaligned countries. A significant factor in why Georgia was so affected by its cyber attack was its extremely limited connectivity to the outside world; Estonia was in a far better position, with a more diverse mesh of connectivity to friendlier neighbors. Submarine cables are also worth noting as a clear point of vulnerability in international transit. There have been a number of accidental submarine cable cuts in the past several years, and a coordinated, willful effort to take those out would be fairly simple to mount and would have significant effect in certain regions.

In the case of Estonia, denial-of-service attacks effectively stopped at the country's IXP and had minimal impact on domestic Internet traffic. In countries lacking IXPs, even domestic traffic may end up routed internationally, at greater expense than if there had been an IXP to broker exchanges before incurring higher international transit costs, and at greater risk of disruption.

It is critical that countries have root and TLD name servers well connected to their domestic IXPs, such that all of their domestic ISPs can provide uninterrupted DNS service to their customers. In the case of ISO country-code TLD name servers, such as those for Estonia's .ee domain, that's relatively easily accomplished, though not yet universally done. In the case of root name servers, it requires

the cooperation and goodwill of a foreign organization, the operator of the root name server, and generally some small investment in infrastructure support for the remotely operated root server. This might amount to an expenditure of some \$15,000 (US) per year, per root server installation within the country.

(It's worth noting that all of the investments required for cyberwarfare defense are equally applicable to general economic development. Just as the cyberwarfare field of conflict is a private-sector space, this, too, is unlike traditional military expenditures. A tank or a bunker is purely a cost center, whereas an IXP or domain name server is a profit center, generating new, concrete, and monetized value for its users from the moment it's established. The return on investment of a newly established IXP is typically less than three weeks, and often less than one week.)

The CERT is a widely employed model for computer and network incident response. CERTs are directly responsible for systems under their own control, and, with other CERTs, collaborate on collective network security. FIRST (Forum of Incident Response and Security Teams), an association of CERTs, brings CERTs and their staffs together to build the most fundamental links in a web of trust.¹ A CERT should also have already established lines of communication with ISPs, law enforcement, and other elements of government concerned with infrastructure security.

Network operators' groups promote community and cooperation between a country's Internet operators and their foreign counterparts. Participation in INOC-DBA (Inter-network Operations Center Dial-by-ASN) and NSP-SEC (Network Service Provider Security) can also aid in coordinating incident response. INOC-DBA is a VoIP (Voice over Internet Protocol) hotline system, interconnecting network operation centers; it uses the networks' own numeric identifiers as dialing numbers so that a NOC operator observing problematic traffic can merely enter the address of the offending network to place a call to the responsible party.² NSP-SEC is an informal organization of security professionals at the largest Internet infrastructure providers: "Membership in NSP-SEC is restricted to those actively involved in the mitigation of [Network Service Provider] security incidents within organizations in the IP transit, content, and service provider community. Therefore, it will be limited to operators, vendors, researchers, and people in the FIRST community working to stop NSP security incidents."³

New members of the "culture of security" come out of academic and training programs (which must be established), intern in a CERT (internationally or domestically), and go on to careers as CSOs (chief security officers) in CERTs, academia, law enforcement, or government. This is fundamentally analogous to the peopling of a national health environment with doctors.

In the U.S., the Department of Homeland Security has included CERTs and information assurance analysts and operators in a new research and development solicitation. In a draft of the forthcoming [as of 1/18/11] solicitation, DHS notes, "While we have a good understanding of the technologies involved in [cybersecurity incident response teams], we have not adequately studied the characteristics of individuals, teams, and communities that distinguish the great [cybersecurity incidence] responders from the average technology contributor. In other areas where individual contributions are essential to success, e.g., first responders, commercial pilots, and military personnel, we have studied the individual and group characteristics essential to success. To optimize the selection, training, and organization of CSIR personnel to support the essential cyber missions of DHS, a much greater understanding and appreciation of these characteristics must be achieved."

CONCLUSIONS

It would be fair to describe these two incidents—Estonia in 2007, and Georgia a year later—as “cyberskirmishing.” The attacks on Estonia amounted to little more than a nuisance, though a quite visible and much discussed one. Georgia had far greater problems to deal with in an armed incursion into its territory, and the Internet was not a factor in that fight.

The difference in responsiveness between the two, however, recommends that the small nation state ought to make investments in Internet defensibility akin to those seen in Estonia:

- Through policy and regulation, and perhaps government investment, foster a robust physical infrastructure.
- Similarly, take steps to ensure a diversity of international connections.
- Encourage (or directly sponsor) creation of one or more IXPs.
- Ensure the domestic availability of DNS resolution, through root servers.
- Foster the growth of a collaborating community of security professionals.

A diversity of interconnections, both international and domestic, facilitated by the efficient peering afforded by IXPs, provides a more robust logical infrastructure, and local DNS resolution further lessens dependence on more exposed international connections. With that technical infrastructure ensured, nations should then foster development of the human infrastructure, the information security personnel needed to anticipate threats, the ability to intercede inventively to restore services, and the ability to support incident forensic collection and analysis. ◻

REFERENCES

1. FIRST; <http://first.org/about/>.
2. Inter-network Operations Center Dial-by-ASN (INOC-DBA), a Resource for the Network Operator Community; <http://www2.computer.org/portal/web/csdl/doi/10.1109/CATCH.2009.36>.
3. NSP Security Forum; <http://puck.nether.net/mailman/listinfo/nsp-security>.

LOVE IT, HATE IT? LET US KNOW

feedback@queue.acm.org

ROSS STAPLETON-GRAY, Ph.D., is research program manager at Packet Clearing House. Prior to joining PCH, he served as an intelligence analyst for the CIA, in information policy positions with the American Petroleum Institute and the University of California Office of the President, and has worked with several IT security start-ups, including as a cofounder of Sandstorm Enterprises.

BILL WOODCOCK is founder and research director of Packet Clearing House, a nonprofit research institute dedicated to understanding and supporting Internet traffic exchange technology, policy, and economics. He entered the field of Internet routing research in 1989 while serving as the network architect and operations director for an international multiprotocol service-provision backbone network. Woodcock has participated in the establishment of more than 70 public Internet exchange points in Europe, Africa, Asia, and the Americas.

© 2011 ACM 1542-7730/11/0100 \$10.00