Panel 5: Norms For Security, Resilience And Integrity in Telecommunications Critical Infrastructure

John C. Mallery, chair and rapporteur, Phillip Hallam-Baker, Comodo Patrick Lincoln, SRI Computer Science Laboratory, David McMahon, Bell Canada, Michael Sechrist, State Street Bank

This panel identified threats to the core telecommunications infrastructure, explained requirements for security architectures, and suggested some strategies and approaches to implementation for assuring trust. Afterwards, it considered several international issues and recommended a number of actions that states and private actors should undertake to secure domestic and international telecommunications infrastructures.

Discussion Questions for the Panel

Threat: What is the model of threat and risk (attack vectors and consequences) unique to core national telecommunications infrastructures?
Security Architecture: What are the requirements for a trustworthy national telecom core?
Strategy: What are the elements of a technical strategy for assuring the telecom core trustworthiness (availability, integrity and confidentiality)?
Implementation: What is division of labor between public and private actors necessary to implement these policy goals?
International Dimension: What aspects of international telecoms infrastructure (e.g., physical hardware or logical operations) require collective action for their protection to assure stable operations of international networks?
Recommendations: What actions should states and private actors undertake in order to secure their core telecommunications infrastructures?

Discussion Questions for the Panel

Threat: What is the model of threat and risk (attack vectors and consequences) unique to core national telecommunications infrastructures?
Security Architecture: What are the requirements for a trustworthy national telecom core?
Strategy: What are the elements of a technical strategy for assuring the telecom core trustworthiness (availability, integrity and confidentiality)?
Implementation: What is division of labor between public and private actors necessary to implement these policy goals?
International Dimension: What aspects of international telecoms infrastructure (e.g., physical hardware or logical operations) require collective action for their protection to assure stable operations of international networks?
Recommendations: What actions should states and private actors undertake in order to secure their core telecommunications infrastructures?

Summary

In the unfolding worldwide cyber security crises, over 120 states are developing offensive cyber capabilities. Although much attention falls on China, the United States and Russia, another dozen cyber powers are more heavily engaged than is generally imagined. Given strong offense dominance and weak defenses, cyber arms races are gathering momentum. Some computer network attacks in support of military objectives have been seen in the cases of Estonia, Georgia, and Iran. Signaling and cyber skirmishes through “hacktivists” or cyber militias now occur quite

frequently. Broad and significant intelligence activity is routine, and lately includes "preparation of the battlefield" with intrusions into critical infrastructures.

In this environment, nation states pursue strategic interests and seek outcomes in political, economic, or military domains. Organized crime has become ever more aggressive and even more capable than many states below the top 20. Although their goals are primarily financial, some criminal elements may seek power and control as surrogates for states that protect them.

For many states, cyber operations offer a new means for global power projection. They may be used for intelligence collection or to achieve military effects. Strategic effects may be realized through attacks on critical infrastructures, particularly power grids, telecommunications and financial systems, but also the oil and gas sector.

The communications sector in modern societies is a complex critical infrastructure. The US Department of Homeland Security defines the sector to include:

Wireline such as fiber optic backbones, undersea fiber optic cables, the Internet, key enterprise networks, cable networks and traditional telephony;
Wireless such as cell phones, cellular data, pagers, and other radio;
Satellite communications for voice and data;
Cable systems providing video programming and internet access;
Broadcast television and radio.

To reduce complexity and because of its criticality, this panel focused on the *telecommunications infrastructure core* (TIC) that consists of:

Terrestrial fiber optic networks;
Undersea fiber optic cables;
Network standards enabling their operation;
Hardware and software supply chains producing the equipment over which they run, including monitoring and control systems;
Key dependencies structures such as the Domain Name System (DNS), edge gateways, the Border Gateway Protocol (BGP);
Carriers, operators and associated processes, including managed services, personnel, vendors, and partners.

The primary criteria for defining this infrastructure as the telecom core was the major bandwidth differential between this class of terabit or 100s of gigabit per second communications and orders of magnitude lower bandwidth of microwave, wireless or satellite communications links. Therefore, disruption of this telecom core severely impairs long distance data links and causes the largest scale downstream consequences.

As the world relies on ever-greater bandwidth, it incurs increasing risks associated with disruption of this global critical infrastructure because so many important political, economic and military activities depend on it. To date, there is no scalable alternative to fiber optic networks, whether terrestrial or undersea. Thus, the undersea cables and terrestrial fiber running across national territories have become a single dimension of potential failure.

Around this telecom core critical for individual nations and the global economy, *strategic technology competition* occurs when states or their surrogates engineer networking standards, hardware, software or managed services for national advantage. To manage this anarchic

competition, we need to develop universalizable norms for system engineering, design certification, procurement, and operations. We need also to establish standards & best practices to reduce opportunities for malicious behavior, enhance stability of the international telecom core and promote orderly and predictable operations of interlinked international networks.

In the NATO CCDCE *'Tallinn Manual' On The International Law Applicable To Cyber Warfare*, rule 5 interprets existing international law to require that: "A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States." Although this means a state should prevent private actors or other states from launching attacks from their territories that rise to the level of "use of force" or "armed attack," it provides no guidance below these thresholds, where most malicious cyber activity occurs today.

The *United States International Strategy for Cyberspace* proposes the following cyber norms for state responsibilities in cyberspace to address the gap:

Internet core functionality relies on systems of trust
- States need to recognize the international implications of their technical decisions
- And act with respect for one another's networks and the broader Internet

Cybersecurity due diligence
- States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse.

Carrying forward discussion of a norm for transparent ICT supply chains with auditable assurance, this panel argued for the similar need to establish *expectations for trustworthy equipment and operational processes in core national telecommunication infrastructures*. Such cyber norms feature transparency of design and separation of duties to ensure vendors and their products are certified to meet assurance standards and receive attestation for fitness for purpose by independent authorities.

On the basis of these considerations, panel proposed the following cyber norm of *State Responsibility For Trustworthy the Core National Telecommunications Infrastructure*.

Cyber Norm: States should seek to foster trustworthiness (availability, integrity, confidentiality) in the operation of their core national telecommunications infrastructure as due diligence to:

- Defend their citizens from malicious actors and violations of privacy;
- Protect their country's national and economic security;
- Isolate and mitigate risks to prevent propagation of adverse consequences for allies, friends, partners, and neighbors.

After this introduction, the panel introduced a *model of threat and risk* focusing on attacker objective unique to core national telecommunications infrastructures that included attack vectors and consequences. In peacetime, attacks on telecom cores are most likely the work of major powers seeking to exfiltrate or intercept wide data streams and defeat large-scale defensive analytics. In wartime, availability attacks are more likely to shape traffic, deny routing, or deny service all together.

Thus, a security strategy seeks to eliminate vulnerability and manage risk in the telecommunications core. Vulnerability can arise for carrier business reasons when low assurance solutions are deployed for cost reasons or when security maturity is low or political interference

occurs. It can also arise when equipment or services are purchased from risky vendors with poor security quality or who are compromised by state actors. Beyond this, low national capacity in technical or policy dimensions may lead to an inability to oversee carriers, difficulty evaluating solutions for security, limited influence over supply chain assurance, and dependency on international companies.

The panel discussed in some detail the technical attack surfaces for the telecom core and adduced a threat model for fiber optic networks that linked attacks on availability, confidentiality, authentication and privacy to countermeasures. It reviewed present day cable threats and concluded there were many opportunities for outages and insufficient attention to resilient architecture, rapid reconstitution, and deterrence.

Security maturity in all organizations associated with the telecom core, including carriers and government overseers is essential for development and implementation of effective security architectures. Since perfect security is rarely possible, a security architecture for the telecom core needs to manage risk. A resilience infrastructure must withstand natural or manmade hazards with minimal interruption or failure. Diverse primary and backup communications capabilities should not share common points of failure. Redundancy must provide multiple communications capabilities to sustain business operations and eliminate single points of failure. Plans and processes for recovery should be in place to restore operations quickly should an interruption or failure occur.

The panel discussed layers and associated security controls in technical security architectures from the physical communications level through electronic equipment, network operations, cryptographic support and networking protocols. A number of technical themes were aired, including topics related to core network operations, filtering of toxic content, software defined networking, and cloud computing. It also examined how secure DNS can improve security of core operations, enable broader more reliable use of cryptography, and enable trust in many new applications.

An industry expert reviewed the current certificate authority infrastructure, including institutions, current operations, response to recent attacks, and identified an emerging industry norm. After an attack on a certificate authority (CA) by Iran and the closure of vendor in the Netherlands because they failed to disclose the breach, the CA industry has moved towards a norm of transparency whereby some CA functions are open for audit.

Strategies to implement a robust security architecture would benefit greatly from research to improve the level of assurance in equipment as well as in operational and maintenance processes of carriers or external service providers. There was some discussion of general US R&D themes for next generation secure networking, including new approaches for achieving hardware and software security, testing and evaluation of systems and reconstitution or recovery of systems.

From the carrier perspective, R&D priorities focused on developing reference security architectures integrating risk management across the telecom core ecosystem that address complex systems of systems and provide strong traceability. The discussion of initiatives with significant payoff included clean pipes to filter malware at the carrier level, strategies for securing cloud computing connected directly to the telecom core, and enabling trusted Internet connectivity. In general, sophisticated carriers are proactive and they are concerned with modeling complex systems, understanding socio-technical interactions, developing indices of cyber protection and creating quantitative evidence-based measures for the effectiveness of security to enable better calculations of return on investment.

A successful implementation of a security strategy needs to achieve seamless coordination between public and private actors. Each has different functional roles in the infrastructure from the supply chain to the operators and service providers and ultimately to the authorities that set standards and provide product certification and attestation. All the while, incentives for industries must remain cognizant of and harmonized with national or supranational regulatory environments.

The panel discussed industry incentives for implementation that included tax incentives and industry participation in oversight of national infrastructures and decisions about public spending for critical infrastructure protection. As a condition of licensing to operate, carriers should be required to produce evidence that they meet national cyber security standards for the telecom core. Regulatory symmetry for national cyber security standards was deemed essential across private and public procurement.

Few cyber security experts are well versed in the economic issues that incentivize IT markets. For example, almost nobody realizes that the WTO Zero-Tariff Technology Trade Agreement (13% of global ICT trade in 2007) denies policymakers use of tariffs as a policy tool to influence the assurance levels of components imported for the telecom core. For policymakers who wish to make domestic market prices reflect risk in components and services, tariffs or insecurity taxes offer a tool that aligns return on investment with information assurance. The panel mentioned, without specific recommendation, four policy options to align risk with price:

Recategorize critical components to enable tariff policy tools;
Implement national assurance standards to block sale or importation of uncertified equipment;
Impose taxes reflecting risk of components as a function of certification level
Use insurance to disfavor low assurance components;
Allocate risk to carriers, for example, by requiring risk insurance as condition of operation.

Another important but longer-term effort involves implementing global transparency of supply chains for hardware, software, and services destined for the telecom core. Transparency needs to span the entire life cycle from design, manufacturing, deployment, operation and maintenance. Equipment needs to be designed for verification and active checking by the customer. And, independent authorities need to certify the assurance levels and attest to the fitness for purpose of components and enterprise processes for procurement and operation.

At the level of Internet hygiene, the panel identified several high leverage areas to contain malicious activity. Assurance of protocols like MPLS, BGP, and DNS are top priorities. Public key infrastructures, their supporting certificate authorities, and identity management infrastructure must be free from compromise for any meaningful security to exist. Naturally, Internet carriers are well positioned to control broad-spectrum malicious activity at scale by implementing existing standards for countering DDOS attacks and quarantining known malware. As an incentive to preserve the cyber commons could, an approach was mentioned that enables distributed traffic shaping for ISPs or ASN numbers based on reputations for poor internet hygiene, bullet-proof hosting, or other antisocial behavior.

Finally, the panel recognized that all nations of the world are dependent on undersea cables and terrestrial fiber optic lines and that a lack of mesh networking somewhere can hurt nations everywhere. Thus, a nation acting alone cannot protect its interests without other nations and companies protecting their own.

Beyond the high-level cyber norm for protecting the telecommunication cores (discussed above), the panel recommended *Norms for State Domestic Due Diligence*:

1. *Develop and execute a security strategy to raise security maturity:*
   a. Threat model – national and international
   b. Security architecture
   c. Security strategy
2. *Maintain a current security architecture:*
   - Separate production and operation from certification and attestation
   - Assure independent evaluation, certification and accreditation
   - Continuously monitor and mitigate threats rapidly
   - Plan for recovery and continuity
3. *Take policy steps to assure:*
   - Manageable complexity in the telecom core
   - Align risk with ability to respond
   - Align equipment cost and total cost of ownership with risk reduction

It also suggested several *International Norms* for states:

1. *Join international efforts:*
   - International Cable Protection Committee
2. *Encourage development of international best practices:*
   - National telecom cores
   - Data sharing and threat mitigation
   - Transparency and certification of equipment
3. *Develop norms reduce high consequence risk:*
   - Protect against disruption of undersea cables during peace time or war
   - Clarify the conditions under international law where network access may be denied or traffic shaped against countries
   - Protect national telecommunication cores, and provide special status for critical elements of the world economy

In the concluding discussion, several questions that linked the panel discussion back to current international dialogues on international cyber norms and CSBMs.

- What telecommunications infrastructure resources require collective international action to protect?
- What scope is there for building trust through collective action to protect such resources?
- Are we likely to be able to build wide international consensus around what requires such collective action, and might this be a way of building trust and confidence?
- Are current international cooperation mechanisms up to the job?

For citation: J. Mallery, rapporteur, Summary for panel 5: Norms for security, resilience and integrity in telecommunications critical infrastructure. Cyber Norms Workshop 2.0, Sept. 2012. http://citizenlab.org/cybernorms2012/