CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

March 2014

Cyber Threat and Response

Combating Advanced Attacks and Cyber Espionage

James Andrew Lewis

Key findings and recommendations include:
—Malicious actors have sophisticated tools and techniques that can defeat current defenses.

—Hundreds of successful attacks occur every month.

—Better cybersecurity will require:

- A dynamic approach to security rather than relying on a checklist;
- More attention to cybersecurity basics;
- New legal remedies to create consequences for cybercrime;
- Test and retest for vulnerabilities in software design and operations;
- Expanded cooperation between private sector and governments;
- Better global governance to create responsible cyber behavior

Introduction

Everyone knows that the Internet has changed how we interact, do business, and share information. The Internet can be an "innovation engine," but the same engine of innovation drives cyber threats to change faster than cyber defenses can react. Cyber threats are complex, dynamic, and network defenses have trouble keeping up with them.

The Internet's original design focused on reliable connectivity, not security. This has not really changed. A quick recap of the situation is that the most devices connected to the Internet are vulnerable, many existing approaches to network security—"black listing," signature-based defenses—are becoming outdated, and most cybersecurity strategies are inadequate. There is a widening gap between offensive and defensive capabilities. Security has not kept up with the threat.

Today's attacks are more sophisticated. So are today's attackers. Cybercriminals now routinely design their malware to evade cybersecurity defenses—the malware behind the recent Target breach was written to avoid notice by most antivirus programs. This "testing" to avoid detection is a common practice. Online

1616 RHODE ISLAND AVENUE NW | TEL. (202) 887.0200
WASHINGTON, DC 20036 | FAX (202) 775.3199

cybercrime black markets make these tools easy to acquire. There is a "pervasive naiveté" among users about security. Opportunistic and motivated attackers, poor security practices, insider threats, and an inability to develop policies and laws that define roles and responsibilities for cybersecurity among government and the private sector, all combine to leave networks vulnerable.

Increasingly, cyberspace is a place where nations create and store value rather than simply transmit information. It is a massively interconnected space that changes at a rapid rate, making static advantage impossible to achieve. Cyberspace is an extension of every other domain that it enables, but it has unique properties that make it difficult to defend.

Threats Are on the Rise

The greatest source of risk in cyberspace comes from groups with the resources and commitment to relentlessly target a company or government agency until they succeed in breaking in and then take value out. These attackers are known as advanced persistent threat (APT). APTs are well-financed, often linked to governments, and possess sophisticated hacking skills that they constantly refine. The most advanced APT groups operate from "sanctuaries" where they face no risk of arrest or prosecution. Most importantly, APTs have found ways to evade most traditional cyber defenses that rely on "pattern matching" to identify and block attacks.

The combination of poorly secured networks and dynamic, innovative attackers has led to a proliferation of attacks. In just the last few months, major retailers and leading banks have all suffered breaches—and these are only the attacks we know about. In 2012, FireEye traced over 12 million communications between botnet command and control servers and infected enterprises.[1] Each of these communications is an intrusion into a network. Cyber attacks continue to increase in sophistication. They now use multiple stage attacks, often stretched out over months, or using new infection vectors (like putting malware on a popular website likely to be visited by company employees). 9,000 new malicious websites designed to snare unwary users are created every day.[2]

Target is a good example of attack sophistication. The attackers exploited a vulnerability in Target's own networks to implant malware that spread to the "point of sale," the machines where people swipe their credit cards at stores around the country. Infecting the point of sale helped evade Target's defenses and internal controls. The malware was written to avoid detection by Target's defenses. Credit card data is encrypted after the card is swiped, but the malware was designed to capture the credit card data in the second between swipe and encrypting and then forward it on to the criminals. The attack combined programming skill and knowledge of business processes to beat an otherwise well-defended company.

APTs can specialize in "zero day attacks," attacks that exploit previously unknown vulnerabilities for which defenders are unprepared. There is a thriving global market for zero day attacks, with researchers in many countries offering their discoveries of unknown vulnerabilities for sale to cyber criminals, governments, or sometimes even the company that produced the software. Zero day attacks are readily available and let APTs use new and undetectable software tools to siphon off cash, intellectual property (IP), or disrupt networks.

The main target for APT action continues to be the extraction of IP, with attackers targeting companies in nearly every industry. Some attacks on company networks last more than three years, with the attacker extracting valuable data the entire time.[3] Others are most like "smash-and-grab," with the attacker getting in and extracting valuable data in a few minutes.

APTs take advantage of a company's own information and use it against that firm. For example, one cyber-criminal group obtained Payment Card Industry (PCI) audits, which assess how well a company secures the networks it uses in credit card transactions. The audits identify weak spots in company defenses, which the hackers used to fine-tune and improve their attacks.

[1] "Global Advanced Cyber Attack Landscape," FireEye, last accessed, September 11, 2013, http://www.fireeye.com/cyber-attack-landscape/.

[2] Malicious websites contain malware that is automatically downloaded when the website is visited. Hackers attract visitors by using common search terms, such as "Gangnam Style" or popular ring tones to get victims to visit the site.

[3] *APT1: Exposing One of China's Cyber Units*, Mandiant, accessed July 1, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Threat Landscape
—Advanced, persistent attackers
—"Upstream" attacks
—"Spear phishing"
—"Zero-day attacks
—Multi-stage attacks

Sophisticated "upstream" attacks are becoming more common. Attackers first go after a company that makes information technology products that other companies use to secure their networks, such as the Secure Socket Layer (SSL) certificates used to authenticate a transaction. They then use the stolen technology to attack dozens or even hundreds of other companies or to deceive end users. It's like breaking into a lock maker to steal the master key and then using the master to open hundreds of doors. The best known example is the attack on RSA, a leading producer of encryption software. RSA was not the real target; the APT attacker broke into RSA to steal authentication technology widely used in financial institutions, defense companies, and other high-value activities. For victims of upstream attacks, the use by hackers of digital credentials that are indistinguishable from the bona fide product can wreak havoc on security.

"Spear phishing" uses a fraudulent e-mail to trick people into downloading malware. The e-mail looks legitimate and will often have an attachment, such as a video or spreadsheet. When the recipient clicks on the attachment to open it, malware is automatically downloaded onto the target network. One successful phishing attack sent e-mails to corporate executives with an attached spreadsheet labeled "Next year's bonuses," an almost irresistible piece of social engineering.

In another case, opening an ".mpeg" movie file attached to the e-mail created a key logger that copied every keystroke made on that machine, allowing the attacker to steal the digital credentials that employees used to authenticate themselves and gain access to the company network. The attacker then used the valid credentials to insert malware that siphoned off specific information. This particular attack affected over 150 high-tech companies.

Attacks can come in stages or waves, each building on the last. APTs will first go after program code or application information that will allow them to access company networks. Once they have access, they will hide their own programs that seek out valuable IP and then exfiltrate it. It's worth noting that in a kind of cyber-Darwinism, it is only unlucky or untalented groups who have been caught or even identified. The most sophisticated attackers are often unknown.

For the APT attacks we know about, almost 90 percent can be traced to China. Chinese APT groups focus on the theft of intellectual property and business confidential information. They lead the world in the illegal extraction of value from others' networks. Changing China's behavior is the key to the cybersecurity puzzle when it comes to intellectual property and confidential business information. Chinese groups are active throughout the world, targeting industries as disparate as aerospace, pharmaceuticals, chemicals, automobiles, and the media. Sometimes these are headline incidents, but most remain outside the public eye.

APTs used to only target companies with high-value intellectual property portfolios. While APTs still go after these companies, they will now target any company with useful information, intellectual property, or money. The victims are everywhere, in almost every industry sector, from small companies to large, and in almost every country.

China is not the whole of the cybersecurity threat, however. Russian APT groups are far more sophisticated, and Russian tradecraft is considered superior to most. Some Russian hackers, for example, make widespread use of encryption; by encrypting the malware they put on company networks, they can make it harder to remove and also defeat the digital forensics work that is used to identify Chinese hackers.

If Chinese APT groups focus their current activities on the theft of IP, Russian and East European groups focus on financial crime. Victims are found in almost every industrial sector. They have been particularly active in targeting companies' CFOs or comptrollers to gain private information on companies' finances, profits, or plans. APT groups are going after very specific information from public companies so they can trade and hedge stock prices using inside information. An area of growing concern is the use of this confidential financial information by Russian groups to manipulate stock markets and prices in ways that are almost undetectable.

> "If you have intellectual property, you're a target. We see this in hospitals and healthcare organizations. We obviously see it in banking. We see it in think-tank organizations. We see it in manufacturing. We see it in energy. Almost every vertical in almost every country, we're seeing major exploits to exfiltrate information, intellectual property and money. So it's gone global."—David DeWalt, FireEye

APTs are opportunistic and inventive. If a corporation is well protected, they will go after their business partners, accountants, or outside law firms, whose defenses may not be as strong, and use these external networks as an alternate way in to get the information they want. Company networks are regularly compromised by attacks that come through outside vendors or third-party service providers—the Syrian Electronic Army penetrated the networks of a third-party service provider to attack and compromise the *New York Times*, for example. Law firms are good targets, a back door to getting confidential corporate information on patents, mergers, or acquisitions.

The threat of APT is not just to information; digital attacks can now have kinetic effects. Physical destruction requires a great deal more coding sophistication and target intelligence than simple information theft, and the cost involved in developing effective attack tools is far higher than the hacking toolkit that forms the majority of current cyber threats, but the number of countries with the necessary skills is increasing. While kinetic effect attacks are still hard to carry out, as they require more resources and skill, an increasing number of APTs have or are acquiring the ability to launch attacks do more than extract value and instead create disruptive or destructive effects that put public safety and national security at risk.

Cyber Defense Has Not Kept Pace with the APT

APTs have the resources, persistence, and skills needed to design complex attacks, overcome most defenses, and avoid detection. Many companies have had their networks compromised; most do not know it. APTs pose a serious threat to cybersecurity as they take advantage of poor coordination and incomplete implementation of basic security controls. Weak defenses mean that the usual pattern for an APT attack is successful penetration and exfiltration of data without the victim even noticing.

We talk about a cyber Pearl Harbor, but it might be more appropriate to reference a cyber "Maginot Line," the expensive French fortifications that the German army simply bypassed in World War II. Many current defensive security architectures have a lot in common with the Maginot Line in that they are stiff, inflexible, and overly complex. Having more layers of similar static defenses does not equate to greater security. A defensive architecture that depends on a static approach using signatures and compliance-based standards is something that hackers will beat every time.

Most companies find out that they have been hacked months after it happened, usually when a third-party tells them. The vast majority of successful attacks require only the most basic techniques, and many attacks could be stopped by uniform use and continuous enforcement of relatively simple hygiene measures. One reason cybercrime is so prevalent is that attackers don't need to work very hard to succeed against most targets.

Most current defenses are focused on "point" solutions, with each company defending itself, and on compliance rather than a dynamic defense, which is both holistic, looking at the entire enterprise, including partners and suppliers, and dynamic, evolving as rapidly as the threat. The static, layered defense approach used by many companies, with different defensive applications corresponding to particular attack vectors, fails to account for social engineering attacks like "spear phishing," or the use of zero day exploits, which can bypass many defenses. A conventional layered defense that relies on multiple layers of signature or pattern matching technologies, such as traditional intrusion detection and preventions systems, firewalls, and gateways, encourages a false sense of security.

Data from FireEye and other companies suggest that APT groups may have compromised more than 95 percent of companies and government networks. The antivirus model for cyber defense is under significant pressure.[4] When antivirus companies first appeared, their business was to look for patterns or signatures that indicated an attack, creating a signature, and

[4] Nicole Perlroth, "Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt," *New York Times*, December 2012, http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html?pagewanted=all.

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036
TEL. (202) 887.0200
FAX (202) 775.3199

scanning files to look for attacks. Over the years, antivirus companies created more signatures and scanned more files. The use of signatures and black listing in antivirus and intrusion detection systems means that we have placed more than 60 million threat signatures at every end point; yet attacks still get through with stunning frequency.

In the past, there was only a few days between the time a new piece of malware appeared and when a signature to identify and block it could be created. In the last few years, however, the speed at which new malware appears and the unprecedented number of attacks has put the traditional antivirus defense model at a disadvantage. Attackers can get past signature lists and file scans and essentially evade a company's entire defense.

APT Favorites
—Static, compliance-based defenses
—Layered, static, point defenses
—Username/password authentication
—Reactive, pattern based defense
—Weak governance

Weak governance compounds the problem of defending against APT. Governance is the rules and understandings that guide cooperative action by companies and governments against APT. Weak governance makes it difficult for companies and government agencies to cooperate with each other in defending against APT. Even unsophisticated attacks can succeed in this environment. The lack of coordination among defenders is a governance problem. Governance would provide the structure and rules that would enable cooperation among defenders and a holistic approach to cybersecurity. The inability to create a governance structure for information sharing among companies and with the government, for example, means that a large number of attacks are not identified, prevented, or remedied. If most network defenses are inadequate, they are also uncoordinated, and weak governance is among cybersecurity's most fundamental problems.

Responding to the Threat of APTs

A quick summary would suggest that our APT opponents are skilled and innovative and our defenses too weak to stop them. This has been the situation for years, but it need not be permanent. While there are no "silver bullets" for cybersecurity, the APT risk can be managed and cybersecurity can be improved through action and cooperation at the international, national, and company level. Our solutions fall into five categories: processes, consequences, technology, governance, and people.

Cyber "hygiene" is the starting point. No company or agency can address cyber threats without first putting in place basic protections. Many attacks could be stopped by uniform and continuous enforcement of relatively simple hygiene measures. One good example of basic controls is Australia's top 35 mitigation strategies.[5] Another is the SANS Institute's Twenty Critical Security Controls for Effective Cyber Defense.[6] These risk vulnerability strategies can help mitigate most of the known threats companies face in cyberspace and can also cut the cost of defense. The mitigation strategies can also help reduce the insider threat to organizations. The National Institutes of Standards and Technology's "Cybersecurity Framework"[7] drafted in response to President Obama's Executive Order of February 2013 provides a long list of things that companies can do to make their networks more secure, and it provides an opportunity to make basic hygiene the norm for cybersecurity.

Hygiene needs to be reinforced by constant network monitoring. This can be something as basic as making sure all security updates are installed on all machines. Consistently checking defenses allows defenders to find weaknesses before a perpetrator can take advantage of them. Security controls are only as good as their application, and information security specialists are continually finding that attacks are more often the result of poor implementation on the part of the victim that they are the use of sophisticated tactics by the attacker. Ultimately, the most sophisticated security strategy will fail if users fail to observe proper hygiene, create shortcuts and workarounds, or neglect best practices.

Be serious about authentication. It's time to retire the venerable password approach to authentication. Companies need to give up using the username/

[5] Australian Department of Defense, Intelligence, and Security, "35 Strategies to Mitigate Targeted Cyber Intrusions," last modified October 2012, accessed July 1, 2013, http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm.
[6] SANS Institute, "The Critical Security Controls," March 2013, accessed September 12, 2013, http://www.sans.org/critical-security-controls/.
[7] "NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments," http://www.nist.gov/itl/cybersecurity-102213.cfm.

password combination to secure anything that is remotely valuable. Programs that can "crack" or guess your password in minutes are widely available in cybercrime black markets, and APT groups have access to even more sophisticated password crackers—many successful attacks exploit weak or stolen passwords. Some kind of improved authentication is essential. There are always objections over cost and on making access more difficult for employees—the same charges can be leveled against putting locks on doors. If a company or agency is still using the venerable username/password combination to secure valuable data, it's like leaving their doors unlocked and unguarded.

Create consequences for APT action. We have come a long way, even from five years ago, when it comes to solving the issue of attribution for various attacks. In many cases (but not all), we can now tell who is responsible. This allows us to refocus our approach when working to create solutions to the problems presented by threats in cyberspace. The ability to attribute attacks provides new opportunities to penalize perpetrators so that attacks can have real and meaningful consequences. Right now, with the penalty for malicious action largely nonexistent, why would anyone stop? There have to be penalties or other serious consequences.

Legal approaches to create consequences are an untapped resource for dealing with APTs. It may be too hard or too risky for an individual company to sue an attacker, but national authorities can begin to use the tools developed for terrorism, nonproliferation, and transnational crime to go after APT—denying visas, restricting the ability to use banks, and indicting those we know have been involved with or have profited from cyber espionage. These are time-tested penalties that we can apply to known APT groups.

The uproar about NSA spying doesn't lessen the value of legal remedies. Many countries engage in cyber espionage. These other countries would not want to haul NSA into court for fear of setting a precedent that could be used against their intelligence agencies. Even if many APT groups have close links to a host government, they are still private individuals who are committing a crime under both the victim's laws and, unlike espionage, under their own national laws, which forbid the theft of financial data or IP. The world needs to stop giving APTs a pass when it comes to cybercrime.

Another possible set of consequences is problematic but a subject of growing debate and interest—the idea of companies striking back at their attackers, sometimes referred to as active defense. Generally, what a company does on its own network to protect itself, including putting false information on its internal network, using a honey pot, or marking its intellectual property to track or control its use, is largely a matter of company policy and national law and does not create liability risks. However, if a company goes outside of its own networks, particularly if it goes onto a foreign network to retaliate, it becomes a matter of international law and a source of liability for the company itself. Moreover, in light of U.S. efforts to encourage countries like Russia and China to cooperate in law enforcement against cybercrimes, it would be hard for American officials to reject a request for cooperation in investigating Americans who are hacking back. Private retaliation that gets out of control and damages innocent third parties creates real liability risk. The temptation to hack back is strong, but companies need to think carefully about their exposure before they take on the risk.

The best way to reduce the urge for private retaliation is for governments to become more assertive in going after APTs. This does not mean declaring war, it means putting to use the full range of diplomatic, trade, and law enforcement tools to create real consequences in an environment where consequences have traditionally been so limited as to be nearly invisible. The alternative is passively accepting victimization.

Take advantage of new technology. There are effective cybersecurity technologies in the market, but new developments offer a chance to close the gap between attack and defense. Big data, cloud computing, and software as a service can be more than slogans. The technologies behind them point to new kinds of cyber defenses. The use of virtual machines to test files before they reach the target network are a promising new approach to using technology, and there are many others that can help us move away from a reactive approach. Standards for dealing with advanced threats and for expanding interoperability among vendors could advance technology in ways never seen before.

Threat mitigation requires robust testing of Internet architectures, applications, and programs to find vulnerabilities. Currently, vulnerabilities are embarrassingly obvious and abundant, often due to

poor development and testing practices. Changing this will require something of a shift in mindset for software developers. One topic for debate is whether better security will also require codification of a more complete liability framework for firms involved in the development and sale of software.

Combine threat information. Currently, companies big and small only know a piece of the cybersecurity puzzle. Right now, "situational awareness" about cyber threats is fractured. The sum of our knowledge is much less than the individual parts of what we know about the threat. If we could aggregate all the information that companies and agencies now hold individually, our knowledge of ATPs and our ability to defend would be significantly greater.

Collaboration on cybersecurity between companies, and between companies and governments, faces legal, commercial, and transactional impediments. These can include antitrust issues, the need to protect brands or proprietary information, restrictions on the ability to share information outside the company when it could affect privacy, and other liability concerns. While the United States has created many mechanisms for enhancing collaboration, these issues continue to impede cooperation and the sharing of threat information. Removing these obstacles will require new legislation from Congress. This will not happen in 2014, but there is a growing desire in Congress to act as risk and damage continue to increase.

On a government level this will require clear delineation of authorities and responsibilities for different federal agencies that clearly define the purposes for which shared cybersecurity information can and cannot be used and provides strong privacy protections. Limited use and tight controls on cybersecurity information are essential. For the private sector, better information sharing will involve changing the mindset about sharing and cooperation in defense by providing liability protection and, perhaps, monetary incentives.

One cybersecurity executive said, "RSA has one of the largest and most important security shows in the world. In 2012, 1,372 security companies showed up in San Francisco for the Conference. If you had asked those 1,372 companies how many of them partner with each other you, the answer would have been close to zero, especially when it is interoperability in sharing compromised data, sharing of intelligence. We need to create formats that allow us to share better amongst the security industry."

We have neither the rules nor the technology in place to allow us quickly and easily to share with others the attacks we have experienced. A single APT may target a dozen companies, but it is unlikely that these companies will talk to each other, especially if they are in different sectors. Sharing information to improve defenses requires a shift in how we think about cybersecurity so that companies see each other as partners in protecting against cyber threats and in managing shared risks.

Strengthen cybersecurity governance. Governance is one of the weakest elements of cybersecurity, a legacy from earlier days when the Internet was small, held less value, and had fewer things connected to it. Moving to mature governance models at both a national and international level will be difficult, but it is a crucial step for dealing with APTs.

The international aspect is particularly important, and cybersecurity requires international solutions to defend global networks instead of just local systems. This will require international cooperation between governments and with governments and companies. Better international governance will require common understandings and norms to create an atmosphere that encourages responsible behavior in cyberspace, and common laws and policies among different nations. Norms and guidelines can help control APTs and create an environment with clear rules that allow for mutual cooperation. They can also help protect basic values like the rights of free speech, privacy, and access to information.

A first step for governance is to identify roles and responsibilities. Some functions—law enforcement, diplomacy, military operations—are clearly governmental, while the private sector can often be more innovative and efficient in business practices. A clearer definition of roles and responsibilities for government and the private sector—and mechanisms for cooperation—will strengthen our defenses. Finding new approaches will require an innovative mindset, a willingness to give up past solutions, and perhaps, formal understandings on private-sector and government roles and responsibilities.

Build the cyber workforce. There are simply not enough people with the defensive skills we need to meet the APT on equal terms. Trained and qualified personnel are needed not only for developing and

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036
TEL. (202) 887.0200
FAX (202) 775.3199

testing security systems and approaches, but implementing them in organizations whose focus may have very little to do with security. Training programs sometimes fall into the trap of using the same checklist approach to cybersecurity that hampers company efforts. A checklist won't make a company secure. These individuals may be the only resource a company will have for security and need to be capable of responding to incidents and thinking on their feet.

Cyber education and awareness goes beyond the IT community. We need to think how to educate employees and managers about cyber risks. In particular, getting corporate boards and the C-Suite to pay greater attention to cybersecurity may be the key to strengthening company defenses. Most corporate boards have a risk management committee; what is needed now is for each of these risk management committees to put cyber risk on the list of what they watch and control.

Move beyond the Maginot Line. Static, compliance-based cybersecurity strategies don't work. Cybersecurity solutions need to keep pace with an inventive and aggressive APT. Security needs to be an ongoing business practice, a mindset that pushes defenses to evolve with the threat.

A dynamic approach requires continuous testing, monitoring, and adjustment of networks and products. It means taking advantage of new technologies for defense. APTs will innovate, and because of this, the physical security model of guns, gates, and guards will not work for cybersecurity.

One way to ensure a dynamic approach is to make cybersecurity a Corporate Board responsibility, preferably as part of a Board's Risk Management Committee. Few risk committees would accept a static approach to managing financial or foreign exchange risk, and the same level of strategic oversight and processes is required for cybersecurity.

Grounds for Optimism—Not Now but Soon

While the problem of cybersecurity and APTs, like any other crime, will never be completely eradicated, it can be brought under control. Cyberspace does not need to be the Wild West. This white paper shows that there are things we can do to address the threat. The challenge is remarkable, but the constant stream of news about breaches and hacking has brought companies and nations to the point where they are desperate for action. Reaching agreement on collective international action is hard and will take time. But individuals and firms can take responsibility for implementing secure practices. Software developers can build security into new products and apps. Transitioning away from a reactive, signature-based security is critical to developing effective security architecture for the future. When the Internet was created, it is fair to say that people had no idea how to secure it (or realized that it needed to be secured). This has changed, as recognition of the threat has grown and as effective solutions, while not implemented, have at least been identified.

The APT threat will continue to evolve in both variety and sophistication, but this threat can be managed and reduced. We do not need to let malicious actors put the Internet in greater peril. Better processes, consequences, technology, governance, and people will let us manage the majority of cyber threats. Advanced persistent threats will remain, but with measures like these, we can control how they develop and manage the risks they present in the years ahead.

Building Blocks for Cybersecurity
—Put in place cyber "hygiene"
—Require better authentication
—Create consequences
—Take advantage of technology
—Build the workforce
—Strengthen cybersecurity governance
—Create dynamic processes for defense

James Andrew Lewis is a senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C., where he writes on technology, security, and the international economy.