ASIS Councils NEWSLETTER

Banking & Financial Services Council October—November 2012

Special points of interest:

- Project Blitzkrieg
- Robert Gates Speaks at ASIS International 2012: Seminar & Exhibits in Philadelphia

Inside this issue:

'PROJECT BLITZKRIEG' PROMISES MORE AGGRESSIVE CYBERHEISTS AGAINST U.S. BANKS

Source: Krebs on Security
October 8, 2012

Last week, security firm RSA detailed a new cybecriminal project aimed at recruiting 100 botmasters to help launch a series of lucrative online heists targeting 30 U.S. banks. RSA's advisory focused primarily on helping financial institutions prepare for an onslaught of more sophisticated e-banking attacks, and has already received plenty of media attention. I'm weighting in on the topic because their analysis seemed to merely scratch the surface of a larger enterprise that speaks volumes about why online attacks are becoming bolder and more brash toward Western targets.

RSA wasn't specific about where it got its intelligence, but the report's finding appear tied to a series of communications posted to exclusive Underweb forums by a Russian hacker who uses the nickname "vorVzakone," which translates to "thief in law." This is an expression in Russia and Eastern Europe that refers to an entire subculture of elite criminal gangs that operate beyond the reach of traditional law enforcement. The term is sometimes also used to refer to a single criminal kingpin.

In early September, vorVzakone posted a lengthy message announcing the beginning stages of a campaign he dubbed "Project Blitzkrieg." This was envisioned as a collaborative effort designed to exploit the U.S. banking industry's lack of anti-fraud mechanisms relative to European financial institutions, which generally require two-factor authentication for all wire transfers. The campaign, purportedly to be rolled out between now and the Spring of 2013, proposes organizing hacker cells throughout the cybercriminal community to collaborate in exploiting these authentication weaknesses before U.S. banks erect more stringent controls. "The goal – together, en-masse and simultaneously process large amount of the given material before anti-fraud measures are increased," vorVzakon wrote. A professionally translated version of his entire post is available here.

RSA said the project is being powered by a version of the Gozi Trojan called "Gozi Prinimalka." The company believes this Trojan is part of family of malware used by a tight-knit crime gang that has stolen at least $5 million from banks already. From its analysis:

"In a boot camp-style process, accomplice botmasters will be individually selected and trained, thereby becoming entitled to a percentage of the funds they will siphon from victims' accounts into mule accounts controlled by the gang.

ASIS INTERNATIONAL
Advancing Security Worldwide®

Security is always excessive until it's not enough.

- Robbie Sinclair

"Take the Challenge: Earn your CPP, PCI or PSP"

Increased professionalism through development.

BLITZKRIEG (cont.)

To make sure everyone is working hard, each botmaster will select their own 'investor,' who will put down the money required to purchase equipment for the operation (servers, laptops) with the incentive of sharing in the illicit profits. The gang and a long list of other accomplices will also reap their share of the spoils, including the money-mule herder and malware developers.

While the campaign is not revolutionary in technical terms, it will supposedly sport several noteworthy features. A novel virtual-machine-synching module announced by the gang, installed on the botmaster's machine, will purportedly duplicate the victim's PC settings, including the victim's time zone, screen resolution, cookies, browser type and version, and software product IDs. Impersonated victims' accounts will thus be accessed via a SOCKS proxy connection installed on their infected PCs, enabling the cloned virtual system to take on the genuine IP address when accessing the bank's website."

vorVzakone also says the operation will flood cyberheist victim phone lines while the victims are being robbed, in a bid to prevent account holders from receiving confirmation calls or text messages from their banks (I've covered this diversionary tactic in at least a couple of stories). Interestingly, this hacker started discussion threads on different forums in which he posts a video of this service in action.

The video shows racks of centrally-managed notebook computers that are each running an installation of Skype. While there are simpler, cheaper and less resource-intensive ways of tying up a target's phone line, causing all of these systems to call a single number simultaneously would probably achieve the same result.

Under "Regulation E" of the Electronic Funds Transfer Act (EFTA) consumers are not liable for financial losses due to fraud — including account takeovers due to lost or stolen usernames and passwords — if they promptly report the unauthorized activity. However, entities that experience similar fraud with a commercial or business banking account do not enjoy the same protections and often are forced to absorb the losses. Organized cyber thieves, meanwhile, have stolen tens of millions of dollars from small to mid-sized businesses, nonprofits, towns and cities, according to the FBI.

ASIS Professional Development

Professional Development Programs:
Nov 12: ASIS Assets Protection Course: Principles of Security (APC I)
Nov 19: Second CSO Roundtable European Security Summit
Nov 26-30: Wharton/ASIS Program for Security Executives Week I
Dec 3-4: Executive Protection
Dec 3-5: 6th Asia-Pacific Security Forum and Exhibition
Dec 17-21: Resilience Management Lead Auditor Certification

Webinars:
Oct 17: Managing an Armed Security Force Synopsis
Oct 23: Achieving ASIS Board Certification - The PCI Journey
Oct 24: Modeling and Simulation for Optimizing Security System Design
Nov 7: Tag You're It! Providing Flawless Customer Service in the Healthcare Security Environment
Nov 14: Excellence in High-Impact Security Education Training
Nov 15: Achieving ASIS Board Certification - The PSP Journey
Dec 12: Tasers in Your Facility: Balance Liability Against Threats

A complete list of events can be found at:

www.asisonline.org

In the News

How to Protect Multi-Facility Enterprises 07/12/2012, Security Technology Executive

Security can be complicated for facilities that have multiple locations across North America. One of the biggest questions security directors face today is whether to standardize the security systems their company will deploy, as large companies begin to see the value in the strategy because it can help lower the overall cost of a system and enable them to manage employee access privileges through a single interface. Several years ago, companies often had one brand of access control system for an office in a small city in the Midwest and another type for a big city office on the West Coast. Aside from the issue of standardizing technology, corporate security professionals will likely face the challenge of helping rural offices understand that security is extremely important, and is not just about protecting assets. Directors can specifically list the requirements for such locations to help ensure a security program is accepted and implemented, but they should also be willing to adapt to the needs of local offices, such as allowing entrance and exit for courtyard areas without requiring card access. There will be budget issues as security directors look to deploy devices, software and other equipment across multiple locations. Also, they will need to future-proof security products to ensure they still have value in five years or more.

Instead of Gun Control: More Private Security 07/23/2012, Bloomberg Business Week

After the deadly shooting in Aurora, Colo., on July 20, Bloomberg Businessweek editor and author Paul M. Barrett opines that instead of falling back on what he views as a tired and unproductive debate about gun control in response to the tragedy, the nation should respond instead by calling for an increase in the use of private security. "If you really want to stop mass shootings in public places, demand that owners of movie theaters, supermarkets, playgrounds, and you-name-the-venue hire armed security guards to keep watch for people dressed in body armor and carrying weapons," writes Barrett. He argues that most major sport arenas, another venue in which massive numbers of people gather together, already conduct searches of patrons for illicit weapons, and that the same should be done elsewhere. Barrett does acknowledge a potential slippery slope, citing the examples of London in the run up to 2012 Olympics and Tel Aviv, Israel as the examples of places where mass violence, or its mere threat, has led to the presence of armed security forces almost everywhere. It is not possible to always prevent every madman hell bent on mass murder, says Barrett, but when we have the ability to do more to protect ourselves, we should take advantage of it.

Punishment Not Effective in Reducing Terrorism 07/31/2012, UPI

According to a study done by researchers at the University of Denver and the University of Maryland, conciliatory tactics are more effective than punishment when it comes to fighting terrorism. The study's authors, the University of Denver's Erica Chenoweth and the University of Maryland's Laura Dugan, developed the Government Actions in a Terrorist Environment -Israel dataset, which identifies counter-terrorism strategies used by the Israelis against Palestinian targets and places them on a 7-point scale ranging from violent acts to conciliatory acts. According to the research, Israel took 18 punishment based actions against Palestinian targets in the average month between 1987 and 2004,

Cyber Security—One of the most intense challenges of our time.

"Foreign Spies Stealing U.S. Economic Secrets in Cyber Space"

Develop a program to respond to allegations or suspicions of fraud in your company!

The FBI reports a rise in bank robberies reported in South Florida for 2012!

"Protect America's Trade Secrets"

- FBI

Rash of suspicious envelopes sent to New York City Banks!

In The News (cont.)

while taking less than eight conciliatory actions. The study found that when lawmakers focused on improving the living conditions for Palestinian residents, the residents were less likely to participate in terrorist groups and terrorism rates dropped.

Hard Lessons
08/01/2012, Security Management

Virginia Polytechnic Institute and State University (Virginia Tech) in Blacksburg,Va., has been through so much since a gunman Seung-Hui Cho, killed 38 people, including himself, and has attempted to learn important lessons to limit another mass shooting in the future. Virginia Tech did use mechanisms such as e-mail to send out information about the shooting, but technology has made instant mass communication far easier since the April 16, 2007, tragedy. Today's notification systems can generally be used with all carriers and most every student has a smartphone. Best practice is to have numerous ways to reach members of the campus with pertinent information, and Virginia Tech's current system includes text messaging, e-mail, message boards, sirens, and desktop alerts, among others. While, every situation will require different directives, such as the message to shelter in place, communication is still a challenge because information on Twitter or a rumor can lead to confusion in the heat of the moment. A new state law requires colleges to have threat assessment teams, and the university has brought together individuals from different departments and disciplines to perform the task of identifying dangerous behaviors. Also, more schools are adopting the approaches of the National Incident Management System (NIMS) and the Incident Command System (ICS) for coordinating activity with local law enforcement in the event of a major incident.

End Users See Benefits of PSIM
08/06/2012, SecurityInfoWatch.com

In this article, James Chong, founder, CTO, and senior vice president of strategic innovation at VidSys, and Don Campbell, vice president of product management for VidSys, share a few ways organizations are using physical security information management (PSIM) software to improve security, safety, and business operations that would otherwise be costly or impossible without it. Using PSIM software, one global Fortune 50 enterprise was able to reduce the number of false alarms being reviewed by 90 percent. The software let the organization track the time and location of alarms so that a video could be reviewed immediately. Prior to implementing the software, all alarms and cameras would have to be reviewed manually to determine where the alarm was triggered. Enterprises also use PSIM software in situations where there have been multiple invalid card swipes on a specific door within a certain period of time to determine whether the card holder and the individual in the video match. The system, when integrated with the HR department, help personnel determine quickly whether or not the person is an active employee. Prior to using the PSIM software, different operators would have to look at each system individually, and would then have to coordinate information and determine whether or not to take further action. The City of Baltimore was able to test its new PSIM software just one week before the start of the inaugural Grand Prix, when the city endured an earthquake and the remnants of a hurricane. The events allowed the mayor to test the system as he reviewed live feeds from helicopters in order to make assessments and decisions about impacted areas -- specifically those

In The News (cont.)

without power. And one prominent university's PSIM software platform helped campus police identify, track, and apprehend five individuals involved in an attempted robbery on campus. The software allowed police to verify a license plate number, immediately pull up the video from the location, and visually identify the suspects. As a direct result, four of the five suspects were criminally charged and prosecutors were able to use the video as part of the investigation.

California Man gets 27 Years in Prison in $50 Million Fraud
08/13/2012, Bloomberg News

A California man was sentenced to 27 years in prison for his role in a $50 million bank fraud that operated in six States and involved 500 victims worldwide, federal prosecutors in Minnesota said August 13. Another person, of New York, was sentenced to more than 22 years behind bars, a Minnesota U.S. attorney said in a statement. U.S. juries convicted the men in February of participating in a ring that bought and sold stolen bank customer data, which they used to open bank and credit card accounts and apply for loans between 2006 and 2011, according to court papers. Among the victims of the scheme were JP Morgan Chase & Co., Wells Fargo & Co., and American Express Co. One of the men was convicted of identity theft, bank fraud, and conspiracy. The other was found guilty of those and other counts including mail fraud and money laundering. Nine other people were charged in the case. Six pleaded guilty and three remain fugitives, prosecutors said. The plot operated in California, New York, Texas, Minnesota, Massachusetts, and Arizona.

Curbing Card Fraud at the Pump
08/31/2012, BankInfoSecurity

Card fraud linked to pay-at-the-pump gas terminals is growing, and that trend will continue until more fraudster convictions are publicized, some security experts say, according to BankInfoSecurity August 31. Meanwhile, in an effort to help prevent fraud, one trade association is testing a system designed to help alert convenience stores and others about potential skimming threats. A fraud expert at Aite said that many card issuers speculate that the increases are linked to crime rings that want to exploit the card data they have in-hand before the U.S. payments infrastructure migrates to chip-card technology, part of a movement to comply with the global Europay, MasterCard, Visa standard. To help combat skimming, the Petroleum Convenience Alliance for Technology Standards (PCATS) is beta-testing a skimming database that logs reports of pay-at-the-pump skimming incidents. PCATS is working with about 10 retail and petroleum brands to collect data that can be used to identify common targets. Once regions or certain terminal brands have been identified as being hit by skimming most often, PCATS notifies other convenience stores and gas stations that are likely to be the next victims.

EMV Flaw allows 'Pre-Play' Attacks on Chip-Enabled Payment Cards
09/12/2012, IDG News Service

Many ATMs and point-of-sale (POS) terminals fail to properly generate random numbers required by the Europay, MasterCard, and Visa (EMV) protocol to securely authenticate transaction requests, according to a team of researchers from the University of Cambridge. The use of defective random number generation algorithms make those payment devices vulnerable to so-called "pre-play" attacks that allow criminals to send fraudulent transaction requests from rogue chip-enabled credit cards, the researchers said in a paper released Septem-

Training...

Make your security training effective to achieve increased awareness across the organization!

"Fraud committed by managers or executives can go undetected for as long as two years"

Check out ACFE's recommendations for preventing workplace fraud!

In The News (cont.)

Operation Card Shop nets 24 arrests for credit card theft!

Cyberespionage: “Companies of all sizes could be targeted for the valuable information they may store or have access to”

The new generation of cold warfare!

September 11. The EMV standard requires the use of payment cards with integrated circuits capable of performing specific cryptographic functions. These cards are commonly known as chip-and-PIN cards, EMV cards, or integrated circuit cards. EMV-compliant devices must generate so-called “unpredictable numbers” (UNs) for every transaction request so card issuers can verify the “freshness” of these requests. Older versions of the EMV specification did not provide clear instructions for how these random numbers should be generated and only required that payment devices generate four different consecutive UNs to be compliant. The researchers found weak UN generation in devices that were easy to predict and thus take advantage of for fraudulent transactions.

Skimming Threatens Debit Card Users, While Fraud Strikes 1 Percent of Credit Card Transactions.
09/12/2012, CardRatings.com

Twice as many credit card fraud cases involve phone or online transactions than retail sales, according to new data from FICO, CardRatings.com reported September 12. However, researchers found that sophisticated counterfeit rings have raised the stakes for merchants over the most recent 20-month survey period. Researchers reported an increase in skimming. ATMs, grocery stores, and automated fuel pumps topped the list of places where criminals use stolen or cloned debit cards. According to a company spokesman, fraud rings usually test stolen cards with smaller online transactions. In a statement to reporters, he described online tests as a “relatively safe” way for thieves to learn whether victims notice extra purchases on their monthly statements. The theory rings true with researchers at J.D. Power and Associates, where the results of an annual customer satisfaction survey showed that nearly a quarter of reported credit card problems involved fraudulent transactions.

Visa to introduce Point-to-Point Encryption Service to Payment Terminals
09/13/2012, Softpedia

At the end of August, Visa revealed its plans to introduce a new point-to-point encryption (P2PE) service called Visa Merchant Data Secure, Softpedia reported September 13. The service, which will be made available at the beginning of 2013, will aim at securing payment terminals and other critical systems across the industry. The P2PE technology will allow merchants to protect sensitive cardholder information by encrypting data within the payment-processing environment. The encryption keys will be guarded by Visa, the gateway, or the firm that acquires the service. According to a member of the Visa Risk Group, the new service is not required yet, but it is a tenet of the PCI Data Security Standard.

Cyber Security News

10 Ways Enterprises Can Battle Malware 07/26/2012, Gov Info Security

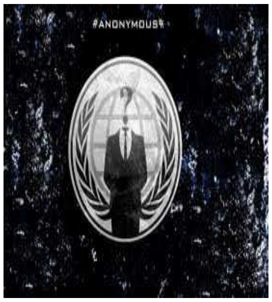
As smartphones and tablets continue to push the bring-your-own-device paradigm in information security, the National Institute of Standards and Technology is reminding organizations that desktop and laptop security remains a top concern. NIST is releasing a revised draft of its Guide to Malware Incident Prevention and Handling for Desktops and Laptops citing the changing nature of the malware threats currently menacing desktop and laptop computers. The revision says today's malware is slower, stealthier, more methodical, and more persistent than malware from several years ago and requires different tactics to combat. The new revision includes numerous suggestions for organizations on how to battle modern malware. The key to doing so is developing and implementing a malware incident prevention plan that will address the specific malware threats faced by their networks today. NIST recommends broadening the responsibility for incident monitoring and prevention by establishing user-based malware awareness programs that help users to be responsible for their machines. Organizations should document their vulnerabilities, as well as prepare and sustain incident response processes for handling malware. Finally, NIST recommends using defensive architecture methods and acquiring threat mitigation capabilities to combat malware head-on.

Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure 07/27/2012, New York Times

U.S. National Security Agency director Gen. Keith B. Alexander says cyberattacks targeting U.S. critical infrastructure rose by a factor of 17 between 2009 and 2011, with criminal gangs, hackers, and other countries driving this increase. Moreover, Alexander warns that the U.S. is ill prepared to repulse a large-scale cyberassault, rating its preparedness as "around a three" on a scale of one to 10. He calls for approval of legislation to grant the government new authority to defend private U.S. computer networks. Rules of engagement for responding to cyberattacks are still under development by the Obama administration, Alexander notes. However, he stresses the need for some automatic defenses, as well as the president's involvement in any decisions about retaliation, given the tremendous speed with which a cyberattack can occur. Alexander confirms that the president has exclusive power to authorize a U.S.-directed cyberattack under current authorities. The Pentagon previously said a U.S. retaliation against an attack on U.S. soil could either come in the form of a counter-cyberattack or a traditional armed response.

Three of Four New Malware Infections in Q2 Caused by Trojans 08/07/2012, TechJournal

More than 6 million new malware samples were created between April and June 2012 alone, a similar figure to the prior three months, according to PandaLabs' Q2 quarterly report. Trojans continued to account for the bulk of new threats created this quarter, followed by worms and viruses. Curiously, viruses continued to decline, dropping from second place in the 2011 Annual Report to third place this quarter. In regard to number of infections caused by each malware category, Trojans once again topped the list, accounting for more infections in the first quarter—76.18 percent, compared to 66.30 percent in the second quarter. The report noted that the figures corroborate existing research showing that massive worm epidemics are now a thing of the past, and have been replaced by banking



Groups like Anonymous have generated highly visible attacks against very large organizations in the last several months.

“About one-half of all Internet Service Provider’s get hit with DDoS attacks each month”

Cyber Security News (cont.)

Trojans and other viruses as the top threats. The average number of infected PCs worldwide stands at 31.63 percent, dropping nearly 4 percentage points from the first quarter. Asian countries take the top three spots of most infections per country, led by South Korea, China, and Taiwan, while nine of the 10 least infected nations are in Europe, with the tenth country being Uruguay. The countries with the fewest infected PCs are Switzerland and Sweden.

> *"Cyber security must be embedded into the systems and networks at the very beginning of the design process"*

Executives Advocate a Military Approach to Cybersecurity
08/13/2012, CNN.com -- Security Clearance

A recent survey of IT executives conducted by the security firm CounterTack is the latest effort in a push by government and private companies to promote the adoption of a more militaristic mindset in cyber security. According to the survey of 100 IT executives at companies with revenues greater than $100 million, 80 percent believed a more military-minded approach to cyber security would benefit business. In CounterTack's case, military-minded means the use of intelligence gathered by the company's security products, which identify and monitor the activity of advanced persistent threats within a network to give systems administrators information about the attack's source, methods, and intentions. "We're talking about that great intelligence real-time situational awareness," said CounterTack CEO Neal Creighton, who points out that in a world where data breaches and network intrusions are effectively inevitable, good intelligence can often be an organization's only source of recourse. Making use of this intelligence requires a very specific skill set and the U.S. government is among the entities pushing for greater recruitment of individuals, often current or former hackers themselves, with these sorts of skills to help narrow the ability gap on the side of IT security.

Cybercrooks Fool Financial Advisers to Steal From Clients
08/27/2012, USA Today

Financial advisers and investment managers are becoming the latest targets of highly targeted spear phishing attacks. As technology has at once cut down on the ability of simple malware to infiltrate and siphon off money from banks and led more people to discuss and authorize money transfers over e-mail, the two have created an opportunity for enterprising hackers. Step one: use social media to identify your target and their financial adviser. Step two: gain control of the target's e-mail account. Step three: e-mail a wire transfer request to their adviser and hope the transfer goes through without anyone becoming suspicious. IDentity Theft 911, which provides identity protection services, has dealt with numerous clients who've been the victims of such fraudulent transfers, several in the tens of thousands of dollars. Most targets of the schemes are medium to small businesses and victims are often unable to recover much if any of their assets. "The shift to personal advisers and individual wire transfers is an indication that the well is running dry for [cyber criminals] with small business and small government," Said Entrust's Jon Callas.

IT's 9 Biggest Security Threats
08/27/2012, InfoWorld

IT security threats have transformed in the last decade, and nine in particular are especially dangerous. First and foremost is the rise of the shadow Internet of massive, corporatized criminal syndicates that mimic the form and function of legitimate multinational companies that have arisen to service the vast black market of cybercrime.

Cyber Security News (cont.)

International organizations such as the Russian Business Network provide hosting and hacking services for criminal clients, while professional malware designers develop specialized, highly targeted malware to sell on open markets that also offer the use of botnets and other services to hackers and criminals. These same marketplaces also serve scammers and con men looking to bring in millions of dollars from phishing schemes designed to steal identities and account information. There are also hacktivists bent on data thefts and cybervandalism targeting their nemesis of the day, while advanced persistent threats engage in evermore sophisticated digital espionage, using custom malware to siphon off intellectual property, state secrets, and military plans from their rivals and allies. Additionally there are the persistent vulnerabilities of the Web itself: Weak passwords, SQL injections, insecure permissions, and vulnerable software that allow malicious actors any number of avenues into a network. There also exists the threat of cyberwarfare backed by nation states, but perhaps the biggest challenge facing IT security is that it remains largely impossible to effectively prosecute and punish the rampant criminality that pervades the modern Internet.

"The only real security that a man can have in this world is a reserve of knowledge, experience and ability"

- Henry Ford

Former Defense Secretary: Intelligence Is an Essential Weapon

By Ronnie Rittenberry
Security Today Magazine

One day after the anniversary of 9/11 and within the same hour of President Obama issuing a statement condemning the attack on the U.S. consulate in Libya that on Tuesday killed four Americans, including U.S. Ambassador to Libya Christopher Stevens, former U.S. Defense Secretary Robert Gates took the stage at ASIS 2012 taking place here at the Pennsylvania Convention Center, delivering Wednesday's keynote address and beginning the day's educational program. He was only a couple of minutes late.

While Gates did not specifically address the breaking news of the attacks, the impetus behind them and the attitudes and violence demonstrated by the Libyan extremists who carried them out was very much part of the former CIA director's theme.

Early on in his speech, Gates anecdotally recalled an incident in the 1980s when he was deputy DCI and was briefed on a plan to launch balloons into Libya that would drop leaflets telling people to overthrow the government.

"I told them to make sure the leaflets specifically said that it was specifically Gadaffi who should be overthrown," Gates said. "I could imagine strong westerly winds carrying those balloons with a generic 'Overthrow Your Government' right across Libya and into Egypt and didn't think [then] President Mubarak would be thrilled."

After that reminiscence, the levity pretty much ended.

Touching briefly on scenes, missions, decisions and political figures spanning the past four-and-a-half decades, during which time he rose up the ranks of the CIA and served as a trusted advisor to eight U.S. presidents, serving as Defense Secretary under two of them, Gates shared his candid insights on world affairs, U.S. intelligence and defense strategies, leadership and his own perspective on security issues in "this messy post-Cold War world [that] does not lend

Gates (cont.)

itself to immutable doctrines."

Recalling the early '90s, when America was "flush with victory in the Cold War" and standing supreme internationally with elements that would later be called "soft power" and the apparent vindication of democratization, Gates stoically noted that those days are gone.
"Twenty years later, the world situation belies that naïve idealism," he said.
If it had not already, that type of idealism came crashing down in an unforgettable way on 9/11, when Gates was still the deputy National Security Advisor (he would be sworn in as CIA director two months later).

"There is an inherent flaw in human nature that happens collectively, and that tendency is to postpone problems until they reach a crisis point," he said. "Before 9/11, there was no Tertullian voice sounding the alarm. After 9/11, the NSA, CIA, FAA and other leading agencies in the intelligence community all had a number of tough questions to answer, but I would argue that so did both political parties," which, through Congress, had fiscally hampered U.S. intelligence operations.
At the end of the Cold War, the CIA still needed more field officers, Gates noted, and, similar agencies responsible for protecting the homeland had likewise suffered cutbacks. Gates cautioned making similar mistakes as the country "careens toward the so-called fiscal cliff" later this election year, when cuts to the military and intelligence agencies are easy (or tempting) to promise.

"Al-Qaeda is on its heels, to be sure," Gates said, "but it's certainly not out. Al-Qaeda is increasingly turning to the alienated and disillusioned for recruits"—individuals, in other words, much like those who launched the rocket attack in Libya on Tuesday.
"Now, 11 years ago today, on Sept. 12, 2001, no one would have predicted that we wouldn't have another attack on U.S. soil," Gates said, noting that it was not a matter of such an attack not being attempted but rather because of the "heightened awareness of our own citizenry."
He added, however, that awareness is only part of the strategy. "We can no more eliminate the risk of terrorist attacks than we can eliminate crime," he said. "We can minimize risk, but we must do so without sacrificing dignity, privacy and rights."

Gates advised a policy of having a minimal military presence in Afghanistan but cautioned against an abrupt exit of U.S. forces because "a pell-mell exit could mean a Taliban takeover and, likely, a renewed civil war there." And such a sudden, wholesale withdrawal could also be something al-Qaeda would use as a rallying point, he said.
Gates rightly noted that Iran's nuclear program is a serious threat, especially to Israel, and he acknowledged that Iranians do have the capacity to disrupt oil shipped in the Persian Gulf and to launch terrorist activities.
"The results of an American or Israeli military strike on Iran could be a catastrophe," he said, "but if there's not an intervention we will very likely face a catastrophe of a different sort: a nuclear-armed Iran."

Gates said the United States needs to pursue partnerships with Persian Gulf nations and make it clear that American leaders do understand their urgency. "After all, we're all in this together, and this is perhaps the most difficult security problem that I have seen since . . . 30 years ago," he said.
China, meanwhile, a country experiencing phenomenal growth, represents another security threat on the international scene, Gates said. That country's economic bullishness has underlying problems that the Chinese government is well aware of, he added, noting that U.S. intelligence forces "expect more belligerences over the months to come."

Threats from all fronts have a new battleground in the cyber realm, Gates said, noting that cyberwarfare does not require a billion-dollar industrial complex to cause harm and, conversely, has "low barriers for entry," where would-be terrorists can easily obtain "toxic tools and deploy them virtually."

Gates (cont.)

Such attacks have the capability of being disruptive and destructive, and while most nation-states would not be behind them because of the likelihood of being found out, terrorist groups who would be otherwise willing to fly themselves into buildings have no such qualms, and the intelligence community thus has to assume such groups will continue trying to use those tools. For that reason, the cyber realm is one of the few areas that is likely to remain budget protected for U.S. forces, he said.

Noting in sum that the security threats are many and challenging, Gates said that forces dealing with such challenges must maintain balance and proportion. Making an embassy into an unapproachable fortress, for example, belies the point of even having an embassy in the first place, he observed. Quoting a line attributed to Frederick the Great—"He would defend everything ends up defending nothing"—Gates said that security breaches inevitably will occur. While he made no direct reference to the breach that took Ambassador Stevens' life hours earlier in Libya, the reference seemed to hang in the air.

Instead, he closed with a passage from Sir William Stephenson's book A Man Called Intrepid: "'Perhaps a day will dawn when tyrants can no longer threaten the liberty of any people. When the function of all nations, however varied their ideologies, will be to enhance life, not control it. If such a condition is possible, it is in a future too far distant to foresee. Until that safer, better day, the democracies will avoid disaster, and possibly, total destruction, only by maintaining their defense.'

"He continued: 'Among the increasingly intricate arsenals across the world, intelligence is an essential weapon, perhaps the most important. Safeguards to prevent its abuse must be devised, revised and rigidly applied. But, as in all enterprises, the character and wisdom of those to whom it is entrusted will be decisive. In the integrity of that guardianship lies the hope of free people to endure and prevail.'"

About the Author

Ronnie Rittenberry is print managing editor for Security Products and Occupational Health and Safety magazines.