U.S. grapples with cyber threats

REUTERS/KACPER PEMPEL/FILES

Businesses, government agencies and critical infrastructure operators face unprecedented challenges in protecting themselves from increasingly sophisticated cyber attacks launched by criminals, hacker activists and foreign governments. To date these attacks have for the most part focused on financial crimes, intellectual property theft and disrupting network operations. Experts and policymakers warn that critical infrastructure, including financial systems, are vulnerable to increasingly destructive viruses that have been identified over the past two years, such as Stuxnet and Shamoon which surfaced in the Middle East. The Obama Administration has asked Congress to give the government new authorities to help protect critical infrastructure from cyber threats, yet lawmakers have yet to pass such legislation. Experts meanwhile warn that adversaries are looking to take advantage . Some top U.S. policymakers and leading experts discussed the challenges they face in protecting the nation from cyber attacks at the 2013 Reuters Cybersecurity Summit, from May 13-15 in Washington.

U.S. cyber bill proponents hope second time's a charm

BY DEBORAH CHARLES AND ALINA SELYUKH
WASHINGTON, MAY 16, 2013

Six months after a U.S. cybersecurity bill died in the Senate, some Obama administration officials and lawmakers are optimistic they can get a new law passed amid heightened public awareness of hacking attacks and cyber espionage.

With top intelligence officials warning that cyber attacks have replaced terrorism as the leading threat against the United States, the White House and lawmakers have spent months discussing how to improve the flow of information between the government and the private sector.

A second go-around for the Cyber Intelligence Sharing and Protection Act (CISPA) was approved by the Republican-controlled House of Representatives in a bipartisan vote on April 18, though the White House has again threatened to veto the bill unless more protections for privacy and civil liberties are added.

Still, senior Obama administration officials say behind-the-scenes talks with lawmakers this time around are constant, more serious and more productive.

"I actually think that the outlook is significantly better than it was last year," the White House cybersecurity policy coordinator, Michael Daniel, told the Reuters Cybersecurity Summit in Washington this week. "What has impressed me has been the willingness of everybody involved to actually continue having those discussions and to continue that extensive level of dialogue trying to find some solutions."

While Daniel cautioned that it is never easy to get the divided House and Senate to agree to anything, he predicted that final cyber legislation might be seen by the fall.

"A lot of us are concerned about getting a good piece of cybersecurity legislation before something really bad happens. As a general rule, legislation that is produced immediately after a crisis is not as good as the stuff that can be done when it's more thought-out," he said.

Last year, the Senate failed to pass a comprehensive cybersecurity bill that combined information-sharing provisions similar to those in the current CISPA with voluntary cybersecurity standards for businesses that control critical U.S. infrastructure.

Since then, President Barack Obama has signed an executive order that directs government officials to set voluntary standards to reduce cybersecurity risk and offer incentives to private companies to adopt them.

A series of high-profile cyber attacks - such as repeated disruptions of the online banking sites of major U.S. banks, or markets plunging on a fake message on the AP Twitter feed about a White House bombing that never happened - have built momentum behind cyber legislation.

SEPARATE BILLS

The Senate does not plan to vote on CISPA, but is expected instead to take up its own cyber-related bills. On Wednesday, Senate Intelligence Committee Chairman Dianne Feinstein, a California Democrat, said her panel was drafting a version of an information-sharing bill.

Congressional aides said staff and lawmakers from both sides of the aisle are constantly meeting on the issue. One Senate aide said it was a collaborative process to agree on multiple key elements to make the overall law stronger.

Representative Mike Rogers, chairman of the House intelligence committee and CISPA co-author, said key senators including Feinstein were "completely all in" on the need to pass a cybersecurity law. The Michigan Republican predicted that House and Senate lawmakers could work out an agreement on at least an information-sharing bill.

"I think we're finally coming to the consensus here that hey, let's pass what we can pass and take another bite. This isn't the end-all cure-all," Rogers told the summit.

He said a meeting was scheduled this week - with more to come - between the House and the Senate to discuss in detail the elements of cyber legislation and see where compromise could be reached, without starting completely from scratch.

Rogers predicted that if a bill could pass through both houses of Congress, Obama would sign it despite the veto threat.

URGENT NEED

Top administration officials have underscored the urgent need for laws that would complement Obama's executive order and help ensure the government and the private sector are on the same page when it comes to threats posed to critical U.S. infrastructure.

Homeland Security Secretary Janet Napolitano said many lawmakers received classified briefings last year on cyber threats, and better education on cyber risks means "we're starting from a much better base" on legislation.

"There's a lot of work going on behind the scenes," Napolitano told the summit. "There are many fewer concerns than there were last time around."

But officials acknowledge that hurdles remain. For example, some senators, like Homeland Security Committee Chairman Tom Carper, prefer a more comprehensive bill.

"While information sharing is an important part of our efforts, it is only one of many elements needed to properly bolster our cyber defenses," Carper, a Delaware Democrat, said in a statement.

To continue reading click here

White House cites progress in cyber talks with China, Russia

BY JOSEPH MENN
WASHINGTON, MAY 14, 2013

The United States has made substantial progress in recent talks on computer hacking issues with both China and Russia, a White House official told the Reuters Cybersecurity Summit.

Michael Daniel, the Obama administration's cybersecurity policy coordinator, said that China has agreed to establish a joint working group with the United States to address Internet security issues such as cyber espionage.

The group will convene for the first time this summer, stepping up communication that had previously been relegated to sporadic discussions or long-running unofficial talks between private citizens from the two countries.

"We're working to set the agenda" for the initial meeting, Daniel said at the summit held at Reuters' Washington offices.

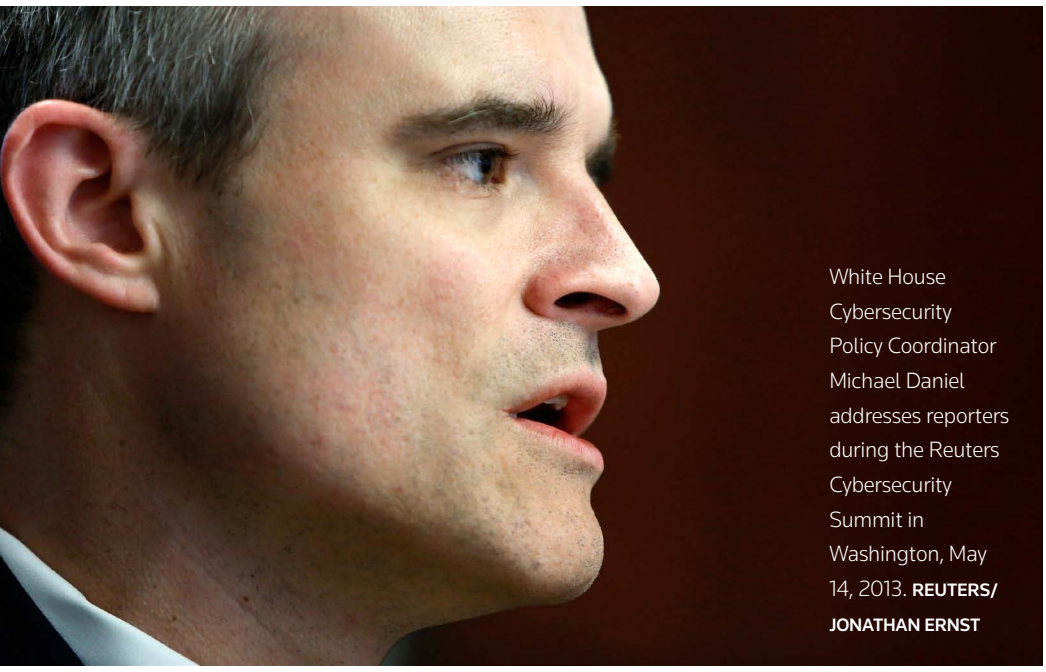
The move comes amid increased pressure on Beijing from President Barack Obama and other U.S. officials to curb theft of digital data, especially from targets outside the traditional spying realms of military and government.

The developments are a rare positive event after a string of unsettling cyber attacks have renewed calls for international agreements on norms of behavior.

"The ability to carry on a dialogue with both the Russians and the Chinese is improving over time," Daniel said. "One of our key goals in this space it is to improve that international cooperation."

With Russia, the talks are an attempt to recover ground from an earlier negotiation that would have established a Moscow-Washington hotline to defuse Internet-security emergencies. That round of discussions had seemed promising for months last year but collapsed at the last minute, officials have said.

Daniel and Obama's national security advisor, Tom Donilon, both worked on the issue during recent travel to Russia, and "some final announcements will come over the next few months," Daniel said, declining to give details.



White House Cybersecurity Policy Coordinator Michael Daniel addresses reporters during the Reuters Cybersecurity Summit in Washington, May 14, 2013. **REUTERS/ JONATHAN ERNST**

Late last year, a classified consensus U.S. intelligence report determined that China was by far the largest thief of economically valuable intellectual property from U.S. companies, taking more than No. 2 Russia and other countries combined.

This year, a report by the private security company Mandiant accused a specific unit in the Chinese army of responsibility for a raft of intrusions.

Mandiant Chief Security Officer Richard Bejtlich told the Reuters Summit that the Chinese army unit changed its tactics for a while after the report was published, but he added that "it appears that these guys are reconstituting."

Though concrete changes might be a ways off, the agreement to direct talks shows that "the Chinese apparently are taking this seriously," said Jim Lewis of the Center for Strategic and International Studies, a cybersecurity expect who has led the U.S. side of the semi-official "track two" talks. "They know they have to do something to placate the Americans."

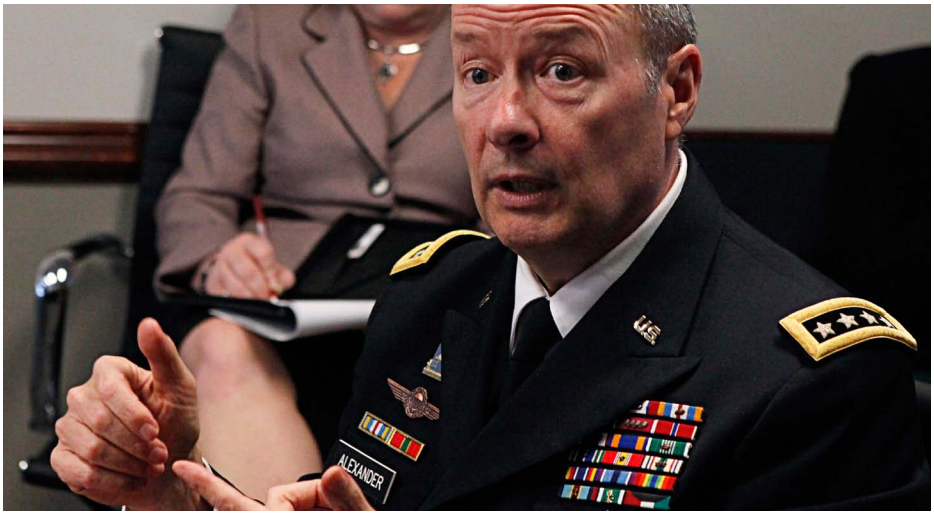
Dmitri Alperovitch, the chief technology officer of security firm CrowdStrike and author of several analyses on Chinese spying campaigns, said that the more formal talks with Beijing would be a "huge step forward" but one not likely to stop state-sponsored Internet spying on their own.

"The next step is to tell them what we're going to do in response" if the behavior doesn't change, Alperovitch said at the Summit. He suggested that the United States could penalize some sectors of Chinese imports by adding tariffs.

Reporting by Joseph Menn in Washington; Editing by Tiffany Wu and Paul Simao

Top general says U.S. under constant cyber attack threat

BY ANDREA SHALAL-ESA
WASHINGTON, MAY 14, 2013



An aide (L) takes notes as U.S. General Keith Alexander, director of the National Security Agency (NSA) and U.S. Cyber Command, speaks to reporters during the Reuters Cybersecurity Summit in Washington, May 14, 2013. **REUTERS/STELIOS VARIAS**

The top U.S. general in charge of cyber security warned on Tuesday that the United States is increasingly vulnerable to attacks like those that destroyed data on tens of thousands of computers in Saudi Arabia and South Korea in the past year.

Army General Keith Alexander, who heads the National Security Agency and U.S. Cyber Command, told the Reuters Cybersecurity Summit that computer networks were under constant attack and billions of dollars worth of intellectual property were flowing out of the country each year.

The result was "the greatest transfer of wealth in history," Alexander said.

"Mark my words, it's going to get worse. The disruptive and destructive attacks on our country will get worse and ... if we don't do something, the theft of intellectual property will get worse," said Alexander, the longest-serving head of the NSA.

The four-star general said he was not aware of cyber assaults against the United States as destructive as the one that damaged computers at Saudi Arabia's national oil company, Aramco, last year. In the South Korean incident, thousands of computers malfunctioned in March, disrupting work at banks and television broadcasters in an attack that officials there blamed on malware used by North Korea.

But Alexander said similar attacks could be seen "in the not-too-distant future" on key U.S. infrastructure sectors, such as public utilities and financial services.

Alexander said that Washington, among other things, needed to engage in more dialogue with China, which the Pentagon has accused of trying to break into U.S. military computer networks.

Top U.S. officials have grown increasingly vocal about threats to U.S. computer networks from China and other countries.

The Pentagon's latest annual report on Chinese military developments accused China for the first time of trying to break into U.S. defense networks, calling it "a serious concern."

China has dismissed as groundless both that report and a February report by the U.S. computer security company Mandiant, which said a secretive Chinese military unit was probably behind a series of hacking attacks targeting the United States that had stolen data from 100 companies.

Alexander said the activities cited by Mandiant were "just the tip of the iceberg" and he favored more "candor" in discussions with China.

"We need China as a trading partner. We need to take a step. We need to let them know that that's unacceptable - stealing intellectual property - and all that's going on as per the Mandiant report," Alexander said.

"I have offered to my counterparts in the (U.S.) Pacific Command and others that at some point it would make sense for myself or my successor to do that," he said.

The general argued forcefully for legislation that would make it easier for the government to work with industry on monitoring private computer networks for signs of intrusion, despite concerns raised by privacy advocates.

But he said the NSA had no interest in reading the emails of U.S. citizens, who by some estimates produce 420 billion emails a day.

"We can protect our networks and protect our civil liberties and privacy," Alexander told the summit.

He said proposed legislation would not allow government agencies to view data that identified individual people, except in specific cases that required special waivers.

Moreover, all reports of intrusions would go to the FBI, the Department of Homeland Security and the NSA simultaneously so that the appropriate agency could take any required action.

Additional reporting by Deborah Charles; Editing by Ros Krasny, Tiffany Wu and Paul Simao

Napolitano says ATM heist sign of cyber crime scope

BY DEBORAH CHARLES
WASHINGTON, MAY 14, 2013

A global network that stole $45 million from two Middle Eastern banks showed how easily financial crimes can be committed and coordinated in cyberspace, and underlined the need for cyber security legislation, U.S. Homeland Security Secretary Janet Napolitano said.

"It demonstrates the kind and scope of financial crimes that are enabled in a network-connected world, particularly by those who have some skill although not necessarily the highest level of skill, quite frankly, but who can coordinate timing and the like," Napolitano told the Reuters Cybersecurity Summit in Washington.

In a crime that came to light last week, hackers infiltrated two bank card processing companies, headquartered in India and the United States respectively, to raise the balances and withdrawal limits on accounts, then withdrew the money from ATMs in 27 countries belonging to Oman's Bank Muscat and the National Bank of Ras Al Khaimah PSC of the United Arab Emirates.

Napolitano, who declined to discuss details of the investigation, said the growing number of cyber attacks on banks has led to a closer relationship between the government and financial institutions to tackle potential threats.

"There is urgency and this is a big problem and legislation certainly would assist us in our efforts," she said, referring to cyber security legislation that has been mired in a divided Congress.

Napolitano, responsible for keeping the United States safe from attacks ranging from cyber crime to what she termed "radicalized home grown plots" like last month's Boston Marathon bombings, said she was most concerned about the "known unknown".

"What I mean by that is particularly in the cyber world where we have imperfect information sharing, where we lack the kind of multi-lateral international reach one would desire, and where are at least known vulnerabilities," she said.

One way to help tackle the vulnerabilities would be legislation that lays out a process to ensure a flow of information in real time so companies will know about possible cyber threats, Napolitano said. In turn, the government can also benefit from information passed about specific types of attacks or intrusions seen by U.S. companies.

The Republican-controlled House of Representatives easily passed the Cyber Intelligence Sharing and Protection Act on April 18, with some support from Democrats. The bill calls for sharing of information but it was opposed by the White House which said it did not include enough privacy and civil liberties protections.

The Senate is working on a number of cyber-related bills. Napolitano said she hoped the Senate and the House could agree on legislation to improve cyber sharing that is supported by the White House. She said there was a lot of work being done behind the scenes on the proposed laws.

While cyber legislation failed to get through the Senate last year, Napolitano said lawmakers had made some progress since then.

"One of the things that happened last year was the education of many members about this field. They didn't know very much, to be truthful," she said.

For continued Cyber-crime coverage:
http://www.reuters.com/subjects/cyber-crime

More congressional hearings on the issue are likely this summer, Napolitano said, but timing for action on the legislation is uncertain. "It's Congress, and they have their own measure of time," she added.

Napolitano also said international cooperation needed to be improved to properly address cyber threats, which she said were growing in sophistication.

"I don't think yet we have the kind of international structure the world should have where cyber is concerned," she said. "That is yet to evolve and unfortunately may only evolve when there is a crisis of some sort."

Napolitano also said the government was studying ways to use its purchasing power to induce software makers to sell more secure products.

"What we are looking at is what kind of incentives could be used to attract companies to use best practices, including in the software arena, and whether there could be procurement preferences," she said.

Napolitano, a former Democratic governor of Arizona, has been mentioned as a possible Presidential contender for 2016 but would not be drawn on the topic. "I have more than enough on my plate to think about," she said.

Additional reporting by Alina Selyukh, Tiffany Wu and Joseph Menn; Editing by Ros Krasny, Jackie Frank and Paul Simao

FBI says more cooperation with banks key to probe of cyber attacks

BY JOSEPH MENN
WASHINGTON, MAY 13, 2013 6:34PM EDT

The FBI last month gave temporary security clearances to scores of U.S. bank executives to brief them on the investigation into the cyber attacks that have repeatedly disrupted online banking websites for most of a year.

Bank security officers and others were brought to more than 40 field offices around the country to join a classified video conference on "who was behind the keyboards," Federal Bureau of Investigation Executive Assistant Director Richard McFeely told the Reuters Cybersecurity Summit.

The extraordinary clearances, from an agency famed for being close-mouthed even among other law enforcement agencies, reflect some action after years of talk about the need for increased cooperation between the public and private sectors on cybersecurity.

The attacks, which have been ascribed by U.S. intelligence officials to Iran, are seen as among the most serious against U.S. entities in recent years. McFeely declined to discuss details of the investigation, including what the banks had been told and whether Iran was behind the attacks.

Banks have spent millions of dollars to get back online and make sure they can stay online. JP Morgan Chase & Co, Bank of America, Wells Fargo, Citigroup and others have been affected.

McFeely said the one-day secrecy clearances are part of a broader effort by the FBI to communicate more with victims of cybercrime, some of whom feel that cooperating with federal authorities carries too much risk of exposure to investor and media scrutiny.

A February executive order from President Barack Obama called for expedited security clearances.

McFeely, who began overseeing FBI cyber and criminal cases last year, said the agency was changing its approach after being "terrible" in the past about keeping targeted companies informed of progress in investigations.

"That's 180 degrees from where we are now," McFeely said at the summit, held at the Reuters office in Washington.

The FBI is working harder at securing international help in combating cybercrime and sabotage, but also needs dramatic gestures, such as espionage arrests of hackers from rival countries, to convince U.S. companies to be more open about their losses, he said.

On the international front, the FBI and Department of Homeland Security have notified 129 other countries about 130,000 Internet protocol addresses that have been used in the banking attacks.

Many of the computers involved in the attacks were infected by viruses before being directed to attack banking websites, and the bulletins have helped other countries to clean some of the computers, FBI officials said.

National Security Agency Director Keith Alexander and other officials have said that the massive theft of intellectual property by China and other countries amounts to the largest transfer of wealth in history. Individual companies, however, have rarely admitted material losses.

McFeely said that part of the problem was that companies have been frustrated at the extreme rarity of overseas arrests or other signs of tangible progress in nascent international talks over the issue. Even some defense contractors contacted by the FBI after breaches are reluctant to share information with agents, he said.

But McFeely said that some indictments have been issued under seal and that arrests would follow, perhaps when hackers identified by name travel outside their home countries.

"The first time we bring someone in from out of the country in handcuffs, that's going to be a big deal," McFeely said.

Reporting by Joseph Menn; additional reporting by Andrea Shalal-Esa and Jim Finkle; editing by Jackie Frank

FBI Executive Assistant Director Richard McFeely (C) speaks at the Reuters Cybersecurity Summit in Washington May 13, 2013. **REUTERS/YURI GRIPAS**

U.S. Homeland Security Secretary Janet Napolitano answers questions for reporters during the Reuters Cybersecurity Summit in Washington, May 14, 2013.
REUTERS/JONATHAN ERNST

U.S. to protect private sector from secret software attacks

BY JOSEPH MENN
WASHINGTON, MAY 15, 2013

The U.S. government will use classified information about software vulnerabilities for the first time to protect companies outside of the military industrial complex, top officials told Reuters this week.

Secretary of Homeland Security Janet Napolitano said that a system being developed to scan Internet traffic headed toward critical businesses would block attacks on software programs that the general population does not realize are possible.

"It is a way to share information about known vulnerabilities that may not be commonly available," Napolitano said at the Reuters Cybersecurity Summit in Washington, D.C.

The information would come from "a variety of sources" including intelligence agencies, she said.

The National Security Agency and other intelligence agencies develop and acquire knowledge about software flaws in order to penetrate overseas networks. Until now, there has been no straightforward way for these agencies to share that classified data with U.S. companies outside the defense sector, even though those companies could become victims of cyber attacks.

The plan is to discreetly share the data through what the government calls Enhanced Cybersecurity Services. Under a February presidential order, those services will be offered by telecommunications and defense companies to utilities, banks and other critical infrastructure companies that choose to pay for them.

Napolitano's Department of Homeland Security will take the information from the NSA and other sources, and relay it to service providers with security clearances. The service providers would then use these "attack signatures" - such as Internet routing data and content associated with known adversary groups - to screen out malicious traffic.

Napolitano's comments were the first disclosure that the screening would also cover attacks on software using methods known to the government that have not been disclosed to the software manufacturers or buyers.

While U.S. intelligence agencies have at times warned software manufacturers, such as Microsoft Corp and Google Inc, or Homeland Security officials of specific, declassified problems, the new system will be machine-to-machine and far more rapid.

It reflects the realization that many espionage attacks from overseas are aimed at the private sector and that future destructive attacks may arrive the same way. (Classified attack signatures have been used to protect defense manufacturers under a Pentagon program.)

House of Representatives Intelligence Committee Chairman Mike Rogers said he was glad about the plan to share more broadly information about vulnerabilities, while maintaining control of the process to avoid tipping off rival countries or criminals.

"This can't happen if you post it on a website," Rogers, a Republican and lead author of a cybersecurity information-sharing bill that has passed the House, told the Summit. "We have to find a forum in which we can share it, and 10 providers serve 80 percent of the market. We have classified relationships with a good number of them."

Among those that have agreed to provide the classified security services are AT&T Inc and Raytheon Co Northrop Grumman Corp said this week it had also joined the program.

The secret but widespread U.S. practice of buying up tools leveraging unknown or "zero-day" software flaws for spying or attacks was the subject of a Reuters Special Report last week, in which former White House cybersecurity advisors said more flaws should be disclosed for defensive reasons.

Michael Daniel, the White House cybersecurity policy coordinator, told the Summit the Enhanced Cybersecurity Services program was still evolving and the type of information shared would change as threats do.

"We want to use the full capabilities that we have to protect as much of the critical infrastructure as we can with that program," he said.

Reporting by Joseph Menn; Editing by Tiffany Wu and Leslie Gevirtz

Cyber attacks against banks more severe than most realize

BY JOSEPH MENN
WASHINGTON, MAY 18, 2013

The series of cyber attacks that repeatedly knocked major U.S. banking websites offline in the past nine months has been more powerful than the general public realizes, government officials and security experts told the Reuters Cybersecurity Summit.

A self-described activist group, Cyber Fighters of Izz ad-din Al Qassam, has claimed credit for the distributed denial-of-service (DDoS) attacks that took down the websites of more than a dozen U.S. banks for hours or even days at a time. Members of congressional intelligence committees say the attacks are sponsored by Iran and show its growing capability in cyberspace.

U.S. banks, Internet service providers and security companies "have had trouble keeping up with the recent DDoS attacks that have had the sophistication and the level of resources that a nation-state entity like Iran can devote to them," House Intelligence Committee Chairman Mike Rogers told Reuters.

"As a result, many key parts of our telecommunications and financial services infrastructure have been stressed to a dangerous level," Rogers said.

In three waves of attacks since September, consumers have reported inability to conduct online transactions at more than a dozen banks, including Wells Fargo & Co, Citigroup Inc, JPMorgan Chase & Co and Bank of America Corp. Banks have spent millions of dollars to fend off the hackers and restore service.

In DDoS attacks, thousands of computers all try to contact a target website at the same time, overwhelming it with meaningless connections until it is rendered inaccessible.

The banks have said little about their frantic efforts behind the scenes to restore websites, and industry groups have generally played down the impact and severity of the attacks.

But Rogers, U.S. Secretary of Homeland Security Janet Napolitano, and FBI Executive Assistant Director Richard McFeely told the summit this week that the progression of intense electronic assaults had spurred new efforts to coordinate among companies, sectors, and governments.

"The increasing frequency with which we have seen that has really increased our relationship with financial institutions," Napolitano told the summit in Washington.

Most of the biggest banks rely on both AT&T Inc and Verizon Communications Inc for Internet bandwidth, with one as a primary provider and the other as backup, industry executives said.

During past denial-of-service attacks, those companies would work closely with their customers and perhaps outside security contractors to help weed out malicious traffic while allowing real customers to connect.

But beginning last fall, as the DDoS attacks grew in volume and as hackers rapidly changed tactics, AT&T and Verizon began swapping techniques with each other as well.

As things stand, "the vast majority of our interaction during distributed denial of service attacks is directly with our customers," said Edward Amoroso, AT&T's chief security officer. "We also communicate with other Internet service providers serving those customers."

The attacks were substantially larger than past denial-of-service campaigns that likewise relied on networks of computers infected by malicious software giving outsiders remote control of their web surfing and other functions. This time, the attackers used infected computer servers capable of delivering more traffic than ordinary personal computers.

Read all summit stories:
http://www.reuters.com/summit/Cyber13

More alarming was the rapid changes in website functions targeted by the machines, including the secure-communications protocols through which banks identify customers, according to George Kurtz, chief executive of security firm CrowdStrike.

"They used to change every few days, but then it was every hour, and then every few minutes," Kurtz said.

"The financial services group are tired about getting punched in the face," he said.

Officials said they were concerned that the attacks could be used as a cover for attempts at theft from bank accounts or to destroy critical data, but they had not seen evidence of that. They worry that the assailants are learning about the banks by monitoring their responses.

Though denial-of-service attacks by themselves do not destroy anything and have historically been seen as a nuisance, the sheer number of compromised computers available for rent to criminals and countries mean that enough firepower could be brought to bear to crash any Internet-facing site, experts said.

As a result, it is impossible to know how much defense is necessary and difficult to know how much is appropriate.

"It is a reality that nobody knows how much DDoS it takes before something starts to break," National Security Agency Director Keith Alexander, also head of the U.S. Cyber Command, told the summit.

Reporting by Joseph Menn; Editing by Tiffany Wu and Tim Dobbyn

Kaspersky plans push for sales to U.S. government

BY JIM FINKLE
WASHINGTON, MAY 15, 2013

Kaspersky Lab, the Russian anti-virus software maker, plans to open an office in the Washington area to spearhead sales to the U.S. government, a bid to offset slowing demand for its programs for consumers.

Kaspersky makes one of the top-selling anti-virus programs in the United States, where it has gained market share in recent years against products from Symantec Corp, Intel Corp's McAfee and Trend Micro Inc.

Yet the Moscow-headquartered company has struggled to make inroads with the U.S. government, one of the world's largest buyers of technology products. Security experts say that the U.S. government typically avoids Russian products out of concern they could have hidden functions that might allow Moscow to penetrate U.S. networks.

Eugene Kaspersky, the company's co-founder and chief executive officer, told the Reuters Cybersecurity Summit that his programs have no such hidden functions. But he said he will build products aimed at the U.S. market in the United States, to assuage any concerns.

"American companies are 100 percent trusted, so we have to prove we are 200 percent trusted," Kaspersky said. "We have to be more American than Americans."

Kaspersky said he will hire U.S. citizens to work in the new office and write, test and compile computer programs.

The company already has a regional headquarters in Woburn, Massachusetts, and an anti-virus lab in Seattle, but does not produce software in the United States.

The new U.S. team will work on an operating system for computers that control electric generators, water systems, factories and other industrial facilities.

Kaspersky said the company is almost ready to test an early version in Russia. He said he hopes the industrial control software will one day account for about a third of its sales.

As global sales of personal computers decline, Kaspersky Lab wants to diversify its portfolio away from PC anti-virus software. Last year global PC sales posted their biggest decline in more than two decades, hurt by a shift to tablets and smartphones.

Kaspersky said falling consumer sales in 2012 crimped overall revenue growth but did not elaborate. The company still has positive revenue growth when sales to businesses are included "but it's a little bit close to flat," he said.

Revenue grew 14 percent in 2011 to $612 million.

Editing by Ros Krasny and Mohammad Zargham

Kaspersky Lab CEO and Co-founder Eugene Kaspersky speaks during the Reuters Global Media and Technology Summit in London June 11, 2012.
REUTERS/BENJAMIN BEAVAN

Summit Speakers

Charlie Croom
Vice President of Cyber Security Solutions
Lockheed Martin Corp

Dmitri Alperovitch
CTO and co-founder
CrowdStrike

Eric Cornelius
Director of Critical Infrastructure and
Industrial Control Systems
Cylance

Eugene Kaspersky
CEO
Kaspersky Labs

George Kurtz
CEO
CrowdStrike

Gerry Cauley
President and CEO
North American Electric Reliability
Corporation (NERC)

Janet Napolitano
Secretary of Homeland Security
Department of Homeland Security

Jeff Moss
Chief Security Officer
Icann

Jeffrey Snyder
Vice President, Cyber Programs
Raytheon Co

Jim Lewis
Senior Fellow
Center for Strategic and International
Studies at Johns Hopkins

Keith Alexander
General, NSA Director, Command,
U.S. Cyber Command
US Cyber Command/National Security Agency

Kevin Mandia
Founder, CEO
Mandiant

Michael Chertoff
Former Homeland Security Secretary
The Chertoff Group

Michael Daniel
Cybersecurity Policy Coordinator
White House

Mike Rogers
Chairman
House Intelligence Comnmittee

Nadia Short
Vice President, Strategy and Business
Development
General Dynamics Corp

Richard Bejtlich
CSO
Mandiant

Richard McFeely
Executive Assistant Director
FBI

Ron Foudray
Vice President, Business Development,
Cyber Solutions
Northrop Grumman

Shane Shook
Chief Knowledge Officer/
Global VP of consulting
Cylance

William Leigher
Rear Admiral, Director of Warfare
Integration for Information Dominance
US Navy

FOR MORE INFORMATION:
Jim Finkle
jim.finkle@thomsonreuters.com
Joseph Menn
joseph.menn@thomsonreuters.com
Andrea Shalal-Esa
andrea.shalal-esa@thomsonreuters.com
Tiffany Wu
tiffany.wu@thomsonreuters.com
Benjamin Beavan
benjamin.beavan@thomsonreuters.com
NIna Andrikian
nina.andrikian@thomsonreuters.com