London 2012 – Safest Games Ever?

# CBRNE Newsletter Terrorism

Volume 43, 2012

## CYBER NEWS


www.cbrne-terrorism-newsletter.com

## Internet may drop for hundreds of thousands in July due to hacker malware

Source: http://abclocal.go.com/kabc/story?section=news/consumer&id=8630663

A few mouse clicks could mean the difference between staying online and losing your Internet connection this summer.

Unknown to most computer users, the problem began with international hackers running an online advertising scam to take control of infected computers worldwide. In response, the FBI set up a safety net months ago to prevent Internet disruptions for those infected users.

But here's where the problem kicks in - that system is to be shut down.

So, the FBI is encouraging computer users to visit www.dcwg.org, a website run by its security partner. The website contains information to see if your computer is infected and explains how to fix the problem.

After July 9, infected users will not be able to connect to the Internet.

Most victims don't even know their computers have been infected, although the malicious software probably has slowed their web surfing and disabled their antivirus software, making their machines more vulnerable to other problems.

Last November, the FBI and other authorities were preparing to take down a hacker ring that had been running an Internet ad scam on a massive network of infected computers. However, officials said if they just threw everyone involved in jail, the victims of the virus would be without Internet service.

"The average user would open up Internet Explorer and get 'page not found' and think the Internet is broken," explained Tom Grasso, an FBI supervisory special agent.

On the night of the arrests, the agency brought in Paul Vixie, chairman and founder of Internet Systems Consortium, to install two Internet servers to take the place of the truckload of impounded rogue servers that infected computers were using. Federal officials planned to keep their servers online until March, giving everyone the opportunity to clean their computers. But it wasn't enough time. A federal judge in New York extended the deadline until July.

Now, said Grasso, "the full court press is on to get people to address this problem." And it's up to computer users to check their PCs.

Here's what the hackers did: They infected a network of probably more than 570,000 computers worldwide. The malware turned off antivirus updates and changed the way the computers reconcile website addresses behind the scenes on the Internet's domain name system.

The DNS system is a network of servers that translates a Web address into the numerical addresses that computers use. Victims' computers were reprogrammed to use rogue DNS servers owned by the attackers. This allowed the attackers to redirect computers to fraudulent versions of any website.

The hackers earned profits from advertisements that appeared on websites that victims were tricked into visiting. The scam netted the hackers at least $14 million, according to the FBI. It also made thousands of computers reliant on the rogue servers for their Internet browsing.

When the FBI and others made the arrests in November, the agency replaced the rogue servers with clean ones. Installing and running the two substitute servers for eight months is

costing the federal government about $87,000.
The number of victims is hard to pinpoint, but the FBI believes that on the day of the arrests, at least 568,000 unique Internet addresses were using the rogue servers. Five months later, FBI estimates that the number is down to at least 360,000. The U.S. has the most, about 85,000, federal authorities said. Other countries with more than 20,000 each include Italy, India, England and Germany. Smaller numbers are online in Spain, France, Canada, China and Mexico.

## Iranian oil terminal 'offline' after 'malware attack'

Source: http://www.bbc.com/news/technology-17811565

Iran has been forced to disconnect key oil facilities after suffering a malware attack on Sunday, say reports.
The computer virus is believed to have hit the internal computer systems at Iran's oil ministry and its national oil company.


Equipment on the Kharg island and at other Iranian oil plants has been disconnected from the net as a precaution.
Oil production had not been affected by the attack, said the Mehr news agency.

However, the attack is believed to have been responsible for knocking offline the websites of the Iranian oil ministry and national oil company.
The Ministry website was back in action on Monday but the oil company site has remained unreachable.
An Iranian oil ministry spokesperson was quoted as saying that data about users of the sites had been stolen as a result of the attack. Core data about Iran's oil industry remained safe because it was on computer systems that remain separate from the net, they added.
The terminal on Kharg Island handles about 90% of Iran's oil exports.
Iran is reported to have mobilised a "cyber crisis committee" to handle the aftermath of the attack and bolster defences.
This committee was set up following attacks in 2010 by a virus known as Stuxnet that was aimed at the nation's nuclear programme.

## Preventing an Olympic-sized Disaster

Source: http://www.infosecurity-magazine.com/view/25302/preventing-an-olympicsized-disaster/

The London 2012 Olympics will be one of the best-protected yet, from a physical security point of view. The UK government has allocated £533m ($835m) for security staff and equipment, and the military has been drafted in to bolster protection. In January, the authorities held a high-profile security exercise in London, including the Royal Marines boarding boats on the Thames.
Fighter jets will be stationed around London, and the Royal Navy's largest ship, HMS Ocean, will be part of a 13,500-person military deployment. While the cost and scale of the operation is smaller than the Beijing Olympics – where some estimates put security costs at US$6.5bn – it is certainly a show of force.

The cybersecurity arrangements for the London 2012 Olympics, however, remain less high profile. There are concerns, among information security experts, that the Games remain vulnerable to sustained attacks from hacktivists, criminal groups, cyber-terrorists or even those who are setting out just to cause mischief.
There are growing concerns, too, that acts intended to disrupt the games could have far-reaching impacts on the wider UK business community, as well as the public. In some ways, information security could be the 'soft underbelly' of the Games. Some security companies have already seen an upswing in fraudulent, Olympic-related websites, especially

those offering cut-price tickets. But, while fraudsters may have already started exploiting public interest around the event, those with more serious intentions may still be marking time.

## Upping Their Game

The London Games face some risks that no Olympics have had to face before. The terrorist threat has, unfortunately, been with the Games since the Munich disaster, and London is certainly a target for some high-profile groups. That threat has now extended, both to the potential use of cyber attacks for terrorist ends, and because the attacks themselves are more powerful, more varied, and more sophisticated.

"While I don't believe London is at any greater risk than previous Olympic locations, the risk is higher for more sophisticated cyber attacks", says David Johnson, senior analyst at Forrester Research. "As we've seen with Stuxnet and other elaborate schemes, the sophistication of both criminals and nation-states is an order of magnitude beyond even 2008."

**"There would be a massive impact if there were a cyber attack that affected the Tube, bringing down the Oyster network for example"**

Steve Bailey, PA Consulting Group

Not only has the technology of a cyber attack changed, so have the motivations. Although some groups will be driven purely by the potential for financial gain, others have more deep-seated reasons to cause disruption. The idea of hacktivism was, at most, embryonic during the Beijing games. Today, though, it is a real concern for all security experts.

"The Olympics are actually a very attractive attack target for political-driven groups or for hacktivism purposes", cautions Chenxi Wang, also an analyst with Forrester. "There aren't many events that have such a large-scale international impact as the Olympics." Any such event, of course, is a draw for the internet underworld.

**"The Olympics are actually a very attractive attack target for political-driven groups or for hacktivism purposes"**

Chenxi Wang, Forrester Research

## Ready, Get Set, Go!

Already, organizations that monitor information security threats have noticed a steady increase in Games-related malware. With tickets for London 2012 in scarce supply, fake ticket sites – and malware or social engineering attacks using Olympic ticket offers to hook in consumers – are a problem.

"The authorities do seem to be doing a lot of preparation, but most of the information coming out appears to be focusing around keeping London running during the Games – around transportation for example", says Steve Bailey, head of operational risk at PA Consulting Group. "They need to move away from that a little bit, towards things like the dangers of social engineering, for example."

As *Infosecurity* has reported before, the London Games organizers were relatively late to set up official ticketing sites, and to publicize official (and safe) internet addresses for the event. This may have given fraudsters and malware writers a head start.

"Ticketing scams have been around for several months", points out Carl Leonard, head of Websense Security Labs. "As soon as ticketing started, malware authors jumped on that bandwagon to capitalize on it. We've seen scam sites offering discounts for specific events for several months. And as we get closer to the event we're likely to see some scandals."

Members of the public are vulnerable on two fronts: scam ticket sites that take payments from consumers – and never send tickets – and those that use the attraction of ticket offers to inject malware on to a users' computer or, potentially, their smartphones. Malware writers are likely to target video sharing, as well as social media sites, especially during the Games themselves.

"When the Games begin there will be highlights on social networks and video upload sites, and there will be scams linking to malicious code", Leonard cautions.

Businesses should act now to educate employees about the risks, he says. In particular, staff should be reminded about the added risks of using insecure networks, such as WiFi hotspots, and that malware may also attack – or spread – via their company smartphones. This could be especially dangerous as the UK Government is encouraging companies to make

more use of home working and remote working, to reduce Games-related congestion.

To combat these additional risks, CISOs and CIOs should act now, if they have not already done so. This means checking that remote and home working systems are up to date, have enough capacity and, critically, that their security measures are up to date. This includes ensuring that employees' computers – especially laptops – have the latest patches, and if they are to be used with sensitive data, support encryption.

"The time to find out your home working system doesn't work is not the first day of the Olympics. Make sure disaster recovery sites are prepared, and ready to go", warns Stephen Bonner, a partner in the security practice at KPMG.

### A Marathon, Not a Sprint

IT helpdesks should also be drilled to handle additional support calls – and to be aware of the risk of hackers posing as employees, in order to take advantage of a busy IT department to obtain passwords or other back doors into systems. CIOs may also want to consider putting critical IT systems into lockdown, to ensure that they work reliably during the event. IT support staff, for example, may find it hard to travel to data centers for maintenance tasks during the games.

"A lot of large enterprises are going into a 'no change' window, as they run up to the Olympics", says Greg Day, CTO for EMEA at Symantec. "You don't want to be making modifications at the same time as preparing for [a large event] happening. For enterprises, if they don't have the right resources up and running now, they will run into that blackout window."

If businesses only have a limited amount of time to prepare, however, then those tasked with defending the Games are already fighting on more than one front.

Organizers will have to contend with distributed denial of service (DDoS) and advanced persistent threat (APT) attacks, as well as a growing use of social media, and social engineering to inject malware into computer networks.

"The world has moved on since Beijing, in terms of the cyber threat", says Jay Huff, EMEA director of HP enterprise security. "Beijing was a more controlled environment. It was much harder for cybercriminals to operate there. But hacktivism is now one of the top scenarios to defend against."

There are concerns, too, that attacks around the games will focus less on information theft or on IT systems, but will instead target control systems and critical national infrastructure (CNI). If successful, such attacks could cause widespread disruption.

### Total Knock-Out

The utilities, systems such as those running ticketing for the Games themselves, and even the UK's core internet infrastructure, could all be targets. But an attack on the public transportation system in and around London could cause some of the most immediate damage and disruption.

"There is no better DDoS attack than [stranding] millions of visitors on the Jubilee line at peak time", warns Stephen Bonner at KPMG. "It is how you prepare for that in practice that matters."

His concerns are echoed by Steve Bailey at PA Consulting Group. "There would be a massive impact if there were a cyber attack that affected the Tube, bringing down the Oyster network for example, or affecting signaling", he says. "The effects would be disastrous, especially around transport hubs like mainline railway stations.

"The networks would also be a good place to attack; it would affect businesses but also people's enjoyment of the Games", Bailey adds. It is here that the interests and security concerns of the London 2012 organizers and businesses in the UK converge. The UK Cabinet Office has already warned businesses of possible disruption to internet connections as a result of Games-related congestion. This could be much, much worse if that infrastructure is also targeted by cyber-crime groups.

Similar concerns also apply to the mobile voice and data networks, which are likely to be more heavily loaded both by visitors and London-based employees working from home, but which also form a significant part of many organizations' backup plans for communications.

"Mobile communications and public networks would be the most obvious targets", says Forrester's David Johnson. "An attack that saturates network links and slows communication to a crawl is one way that such an attack could disrupt internet infrastructure."

That is why, practically speaking, the business and IT security community needs to follow the lead of the Games organizers: plan, test, and test again.

## Slowing time as a way to counter cyberattacks

Source:http://www.homelandsecuritynewswire.com/srdisasters20120503-slowing-time-as-a-way-to-counter-cyberattacks

Researchers offer a new way to deal with cyberattacks on critical infrastructure like power and water utilities and banking networks: slow down Internet traffic, including the malicious code, when an attack is suspected; this would allow networks time to deal with the attacks

One of the striking special effects in the film *The Matrix* occurs during the scene in which Keanu Reeves' character Neo, sways and bends to dodge bullets as time appears to slow to a crawl. Now, that scene has inspired researchers to develop a way to deal with cyberattacks on critical infrastructure, like power and water utilities and banking networks.

The idea, developed by University of Tulsa engineers, is to slow down Internet traffic, including the malicious code, when an attack is suspected. This would allow networks time to deal with the attacks.

This is accomplished by having an algorithm send hyper-speed signals ahead of the malicious data packets in order to mobilize defenses. "Slowing the malicious traffic by just a few milliseconds will let the hyper-speed commands activate sophisticated network-defence mechanisms," according to Sjeet Shenoi of Center for Information Security at U Tulsa.

The core defensive capabilities offered by hyper-speed signaling include distributed filtering, teleporting packets, quarantining network devices, tagging and tracking suspicious packets, projecting holographic network topologies, and transfiguring networks.

Hyper-speed signaling would help thwart cyberattacks, but it is likely to be expensive to implement. The reason for the expense, and anticipated resistance to the countermeasure, is that hyper-speed signaling would require a reserved, exclusive data path for the command and control signals, something that could be seen as an expensive waste of capacity.

Added to this is the need for more buffers and storage. When an attack is sensed, and tainted traffic is slowed down, that data needs to be held somewhere or crucial data may be lost.

Lastly, the core defensive measures offered by hyper-speed signaling would require additional programming to install the countermeasures into the routers, and to protect targeted devices on the network, such as pump controllers, power grid relays, and cash machines.

Hyper-speed signaling is only as good as the threat sensors on which it depends. The sensors might detect malware disguised as legitimate traffic if the virus signature is known, much the way typical anti-virus programs work now. It will fail, however, to identify variants or new malicious code it has never seen before.

This presents a problem in itself. For the hyper-speed signaling paradigm to be effective, it may mean slowing Internet traffic permanently. This is not likely to be a well-received option.

Another detection option, funded by the U.S. Department of Energy and DHS, has been developed by researchers at Dartmouth College in New Hampshire in conjunction with the University of Calgary, in Alberta, Canada. Led by Jason Reeves of Dartmouth, the team has developed a way for infrastructure to monitor itself.

Dubbed Autoscopy, the monitor is an experimental host-based intrusion detection mechanism that operates from within the kernel and leverages its built-in tracing framework to identify control-flow anomalies, which are most often caused by rootkits that hijack kernel hooks.

Autoscopy monitors the kernel, which is the core code of a computer operating system. "We detect changes in the sequence of code the program runs, ones often introduced by malicious programs," Reeves says. Autoscopy can also run verification on the operating system

code to determine wehether it has been altered by malware.

Autoscopy could also trigger the hyper-speed signaling countermeasures.

*— Read more in Daniel Guernsey et al., "Implementing novel reactive defense functionality in MPLS networks using hyperspeed signaling," International Journal of Critical Infrastructure Protection 5, no. 1 (1 March 2012): 40–52 (DOI: 10.1016/j.ijcip.2012.02.001); andJason Reeves et al., "Intrusion detection for resource-constrained embedded control systems in the power grid," International Journal of Critical Infrastructure Protection (in proofs; available online 10 February 2012)*

## Travelers' laptops infected through fake software updates in foreign hotel rooms

Source: http://www.homelandsecuritynewswire.com/dr20120511-travelers-laptops-infected-through-fake-software-updates-in-foreign-hotel-rooms

The Internet Crime Complaint Center (IC3) reports that recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while establishing an Internet connection in their hotel rooms.

Recently, there has been a surge in instances of travelers' laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to setup the hotel room Internet connection and was presented with **a pop-up window notifying the user to update a widely used software product**. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available.

IC3 notes that the FBI recommends that all government, private industry, and academic personnel who travel abroad take extra caution before updating software products on their hotel Internet connection. Checking the author or digital certificate of any prompted update to see if it corresponds to the software vendor may reveal an attempted attack. The FBI also recommends that travelers perform software updates on laptops immediately before traveling, and that they download software updates directly from the software vendor's Web site if updates are necessary while abroad.

Anyone who believes they have been a target of this type of attack should immediately contact their local FBI office, and promptly report it to the IC3. The IC3's complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration. The complaint information is also used to identify emerging trends and patterns.

## How Cloud Computing Can Benefit Disaster Response

By Valerie Lucus-McEwen

Source:http://www.emergencymgmt.com/disaster/How-Cloud-Computing-Can-Benefit-Disaster-Response.html

As technology continues to redefine emergency management practices, the process of incorporating new concepts into daily practice and planning can be confusing. This is especially true if the concept sounds mysterious and cryptic — cloud computing often sounds complex and bewildering.

The truth isn't nearly that exciting. Cloud computing is more like regressing to the early days of network design. The "cloud" in cloud computing was the symbol network engineers used to illustrate unknown domains and large networks of servers located elsewhere. Using the power of other computers somewhere

on the Internet — that's what cloud computing is all about.

"Cloud computing is just hosted computer services," said Pascal Shuback, a program coordinator for the King County, Wash., Office of Emergency Management. "It is simply using the power of other computers on the Internet."

Emergency managers use a cloud every day without thinking twice to: check email, collaborate with applications like SharePoint, access social and professional networks, watch videos on YouTube, or use almost anything from Google.

Cloud computing is not new. What is new is how it's being applied. What it can do for emergency management is make the job a lot easier.

Nick Crossley, manager of emergency management and mission continuity for the University of California, Davis, uses Microsoft SharePoint as a collaborative planning tool for events on campus. "I can set up discussion boards, share documents or resource lists," he said. "I can control access to it, and all the players in any event or incident can access it anytime, from anywhere, on or off campus."

Commercial incident management software is also in the cloud. "We used WebEOC as a cloud for communication and emergency response between all the local, regional and state emergency management," said Daryl Spiewak, former emergency, safety and compliance manager for the Brazos River Authority in Waco, Texas.

## The Advantages

Like everything else, there are pros and cons to delivering services via cloud computing.

One big advantage is the cost. The individual user needs only a terminal/monitor/modem with some limited local storage and access to the Internet. Commercial software packages vanish in favor of subscriptions to the programs or services needed. The agency doesn't need a room full of servers, and IT departments shrink because the data center doesn't exist.

The end-user experience is certainly less complicated. Compatibility problems decrease, because software updates are always current. Dependability increases because services are maintained and available remotely 24/7, no more waiting for desktop support. Profiles remain consistent across all devices, and "intelligent assistants" (think Siri) can customize needed information.

There is a growing niche market for specific industries. A service from Clio lets lawyers manage their practice and communication with clients from the cloud. Oxford University in England maintains a service to give academic researchers a space for long-term retention of their research data. Autodesk has cloud-based tools for designers. The Electronic Medical Records initiative replaces doctors' charts with terminals that allow them to keep track of medical treatments regardless of a patient's physical location.

## Now the Downside

As idyllic as it all sounds, there are concerns about migrating to cloud computing, like bandwidth. Think of bandwidth as the Interstate Highway System. The roadway is the network; the wider the roadway, the more cars (or data) can travel along it; more roadways (networks) mean more options for cars (and data) to get from one place to another. We have the interstate; we don't have the city streets. The downside is that public infrastructure — physical or virtual — isn't a high priority in the U.S. these days.

Another concern is maintaining connections to a cloud. If the link is severed because of a power outage, software crash, or an earthquake or hurricane taking out the local infrastructure, and

the Internet can't be accessed, neither can the data or applications stored there. Case in point being the Microsoft Azure cloud service failure on Feb. 29 that left customers worldwide without access for several hours to several days. This problem is easier to solve: The answer is collaborating clouds. Just like there are failover procedures in data centers, there will be failover clouds.

Security is one of the chief roadblocks to implementing cloud computing systems, certainly for government agencies or any agency receiving federal funding. Some of that may be resolved with the Federal Risk and Authorization Management Program (FedRAMP), which will provide a standardized cloud certification process across the federal government and is set to be launched in June. It is hoped that FedRAMP can address some of the more frustrating complications. For example, Los Angeles excluded its law enforcement departments from the city's new Google cloud-based email system, because of claims that the company couldn't comply with the FBI's Criminal Justice Information Services policies.

Thin notebooks with Internet access can be taken anywhere, used anywhere and because they don't contain much data, can provide a level of security that doesn't exist today. Cloud computing would end the stories about laptops with classified or unencrypted information being stolen, like the ones that were taken from NASA last year that contained command and control codes for the International Space Station.

Regardless, the biggest issue for deployment is simply selling people on the concept. There are IT techs, agencies and ordinary people unwilling to move data and applications to some remote location they can't see or touch. Whether it's a concern about privacy, distrust or just plain stubbornness, keeping files and programs in a cloud requires a shift in mindset — like the one that pushed the widespread adoption of the Internet. And that might take some time.

## Virtual Mission Continuity

For emergency management, cloud computing's biggest advantage can be summed up in three words: virtual mission continuity.

Cloud computing reduces concerns about whether the data center will survive a disaster. Businesses and agencies are good at copying and backing up data, but the real challenge is restoring the applications to keep essential services and critical functions online. Entire servers, including systems, applications and data can be copied, backed up and be ready to activate in another data center in a matter of minutes.

Employees can be sent to a location that has Internet access and it is all still there — accurate as of the moment the disaster happened. Writing most of the devolution section of a continuity of operations plan — how the agency will transfer essential functions and responsibilities to personnel at a different office or location (and back) — becomes a no-brainer. The best part is that cloud computing is equally available to a small agency or mom-and-pop business as it to big ones.

"One of the significant benefits of using the cloud is that you can distribute your personnel," said Gavin Treadgold, former director of the Kestrel Group, a risk, continuity and emergency management consultant group. "It makes it quite a bit easier to have remote personnel contributing without the logistical overhead of bringing them into a disaster zone."

Another mission continuity solution is telecommuting. "The cloud is also helpful when your team, which is normally in a single building, is spread around residential homes or suburban offices," Treadgold added.

Applications and data house in a cloud enable employees to work from remote locations. It removes the burden of running applications on a home computer, permits virtual collaboration of documents and allows real-time communication via instant messaging or programs like Skype.

And isn't it a short jump from that to a virtual EOC? As universal broadband access becomes commoner, an activated EOC can be established in minutes and operated from multiple remote locations simultaneously. It maintains the flexibility and scalability inherent in incident management systems, and makes it easier to send and receive data or visual feeds from the field.

Emergency managers pride themselves on being flexible and resourceful. Cloud computing is a tool that can enhance the primary mission of ensuring that communities survive disasters. It offers increased access to resources

and faster response.
"The cloud is going to change the whole mentality of emergency management," Shuback said. "Responders can be anyone with connectivity, the public included. We can regionalize our capabilities and create virtual operation support teams composed of the people able to support an event, and it doesn't matter where they are."

***Valerie Lucus-McEwen*** *is a certified emergency manager and certified business continuity professional. She also writes the Disaster Academia blog for* Emergency Management *at* www.emergencymgmt.com/academia

## Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad'

Source:http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.T7y8aVKaXAI

Al Qaeda may be turning its destructive attention to cyber-warfare against the United States. In a chilling video, an al Qaeda operative calls for "electronic jihad" against the United States, and compares vulnerabilities in vital American computer networks to the flaws in aviation security before the 9/11 attack.

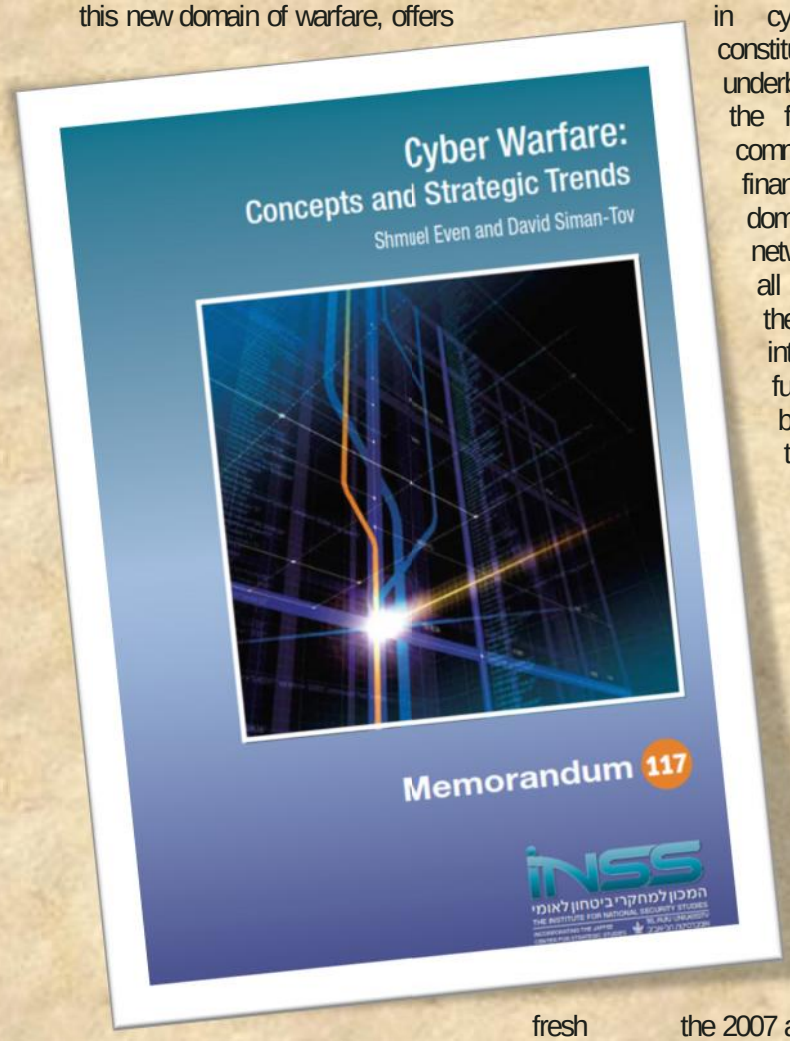

The al Qaeda video calls upon the "covert mujahidin" to launch cyber attacks against the U.S. networks of both government and critical infrastructure, including the electric grid. The video was obtained by the FBI last year, and released today by the Senate Committee on Homeland Security and Governmental Affairs.
"This is the clearest evidence we've seen that al Qaeda and other terrorist groups want to attack the cyber systems of our critical infrastructure," Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman, I-Conn., said in a statement.
"This video is troubling as it urges al Qaeda adherents to launch a cyber attack on America," said Sen. Susan Collins, R-Maine, the ranking member on the committee. "It's clear that al Qaeda is exploring all means to do us harm and this is evidence that our critical infrastructure is a target."
The national security community says the threat of cyber attack is real, and the gap between terrorist aspirations and capability is closing. The senior intelligence official at Cyber Command, Rear Adm. Samuel Cox, has said al Qaeda operatives are seeking the capability to stage cyber attacks against U.S. networks and terrorists could purchase the capabilities to do so from expert criminal hackers.
Increasing evidence also suggests that Iran is looking to commit cyber attacks against the United States, according to testimony last month

before the House Committee on Homeland Security. Iran's sponsorship of terrorist groups takes on a new dimension in cyberspace, where it could develop a powerful cyber weapon and pass it on to a terrorist group.
Lieberman is using the al Qaeda video to underline what he says is the need for new legislation..
"Congress needs to act now to protect the American public from a possible devastating attack on our electric grid, water delivery systems, or financial networks," he said. "As numerous, bipartisan national security experts have said, minimum cyber security standards for those networks are necessary to protect our national and economic security. That is why the Senate needs to act on our bipartisan Cyber Security Act that requires minimum security performance requirements for key critical infrastructure cyber networks."
The Homeland Security Committee says the Department of Homeland Security received more than 50,000 reports of cyber intrusions or attempted intrusions since October, an increase of 10,000 reports over the same period the previous year.

## Cyber Warfare: Concepts and Strategic Trends

Source: http://www.inss.org.il/upload/%28FILE%291337837176.pdf

Cyberspace is a new domain of warfare that in recent years has joined the traditional arenas of land, sea, air, and space. The study that follows describes the unique characteristics of this new domain of warfare, offers




fresh interpretations of familiar concepts, and surveys landmark events and organizations in the field of cyberspace in Israel and abroad. Modern nations and advanced militaries around the world are intensifying their activities in cyberspace, which simultaneously constitutees a source of power and a soft underbelly. The infrastructures critical for the functioning of a state (electricity, communications, water, transportation, finance, and so on) all rely on this domain. Military command and control networks depend on cyberspace, as do all the most advanced technologies of the modern battlefield, such as intelligence gathering, processing and fusion systems, satellite use on the battlefield, use of autonomous fighting tools, real time integration of sensors to identify targets with fire systems, and more.
As an arena of warfare, cyberspace presents some unique features, including the ability to operate quickly, in thousandths of seconds, against enemies located far away, without risking the lives of combat personnel. The unique features of the domain also make it attractive for confrontation in the intervals between conventional wars. One may distinguish between confrontations in cyberspace (such as the 2007 attack on Estonia, attributed to Russia) and wars in which attacks

in cyberspace are but one component in a war alongside other forces (such as Russia's attack on Georgia in 2008). Furthermore, one may distinguish between attacks taking place in cyberspace (attacks on computerized systems) and the use of cyberspace as a means to damage the functionality of machines operating in the physical domain, e.g., the 2009 cyberspace attack on Iran's nuclear program. This event (the Stuxnet virus attack), which demonstrated the great potential impact of cyberspace weapons, was formative in the development of cyberspace as grounds for warfare. It appears that from now on, cyberwar will likely play a part in every modern war. Indeed, both cyberspace attacks that have occurred and processes undertaken by states to prepare themselves in this domain indicate that the cyberspace arms race has already started. As part of this race, a number of states (the US, Great Britain, France, Germany, China, and others) have in recent years established offices and headquarters dedicated to cyberspace as a domain of warfare, and security strategies for cyberspace have been formulated. At the same time, states are also faced with considerations regarding the constraints of cyber attacks and the risk of exposure to counterattacks, especially because defenses are still not sufficiently strong. In addition, non-state elements such as terrorist organizations are liable to use cyberspace to launch attacks, once they achieve the capability of causing severe damage. In tandem, there is growing international recognition that it is necessary to defend cyberspace and regulate its activities – similar to regulation in other realms. This type of regulation can be achieved through inter-state cooperation, adaptation of international law to cyberspace, and formulation of a compelling international treaty. Progress thus far has been slow, certainly not in pace with developments in cyberspace. In the Israeli context, information technologies and cyberspace play a decisive role in Israel's qualitative superiority in terms of its economy and security. Cyberspace is crucial to Israel's society, the bond between the government and the population, and Israel's connections with the world at large. Even more so, it plays a critical role in Israel's national security, especially given the developing cyberspace threats, Israel's information technology advantage, and the potential cyberspace implications for the modern battlefield. All of these dimensions oblige Israel to accelerate its efforts to improve defense of its cyberspace and contribute of its capabilities to the defense of cyberspace on a global scale.

This research was conducted in the framework of the INSS Program on Cyber Warfare, headed by Prof. Isaac Ben-Israel and Dr. Gabi Siboni and supported by the Philadelphia-based Joseph and Jeanette Neubauer Foundation. The authors would like to extend their thanks to Dr. Amos Granit, Head of the Institute for Intelligence Research in Military

Contents

Intelligence, for his constructive comments, and to Patrizia Isabelle Duda for her contribution to the memorandum.

This study is published with the assistance of the gift of the late Esther Engelberg.

**NOTE:** You can download the full Memorandum at the Newsletter's website – "CBRNE-CT Papers" section.

## Powerful 'Flame' cyber weapon found in Middle East

Source: http://www.msnbc.msn.com/id/47590214/ns/technology_and_science-security/#.T8TrB1KaXAm

Security experts have discovered a highly sophisticated computer virus in Iran and other Middle East countries that they believe was deployed at least five years ago to engage in state-sponsored cyber espionage.

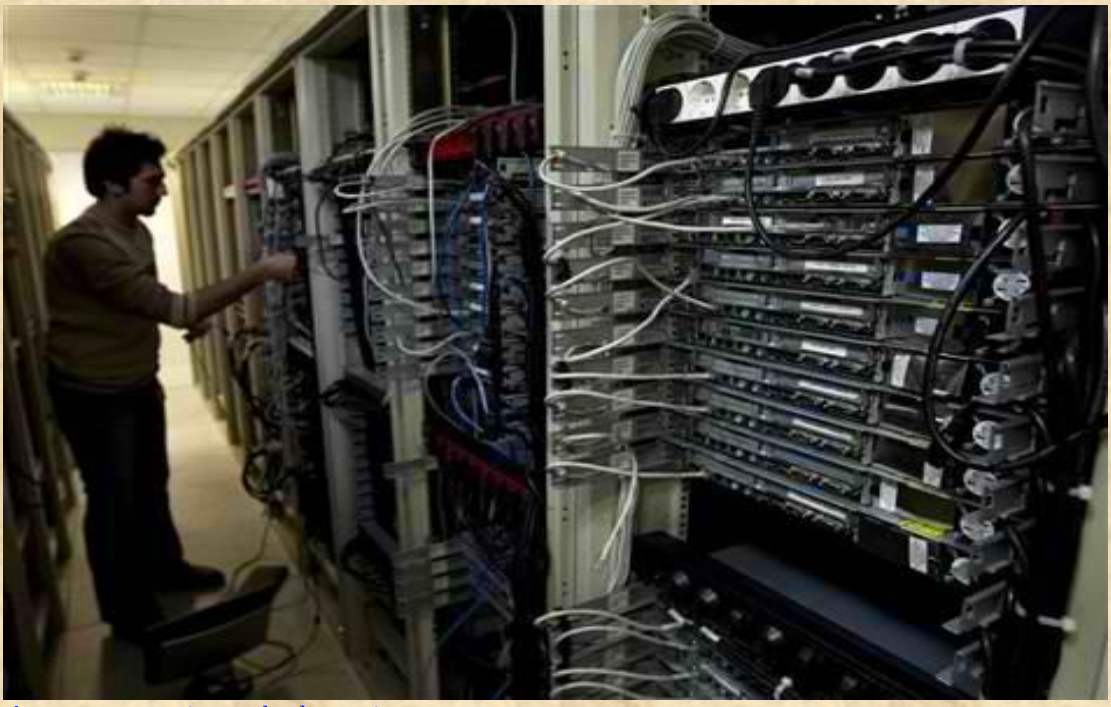
Evidence suggest that the virus, dubbed **"Flame"** may have been built on behalf of the same nation or nations that commissioned the Stuxnet worm that attacked Iran's nuclear program in 2010, according to Kaspersky Lab, the Russian cyber security software maker that claimed responsibility for discovering the virus.

Kaspersky researchers said on Monday they have yet to determine whether Flame had a specific mission like Stuxnet, and declined to say who they think built it.

Iran has accused the United States and Israel of deploying Stuxnet.

Cyber security experts said the discovery publicly demonstrates what experts privy to classified information have long known: that nations have been using pieces of malicious computer code as weapons to promote their security interests for several years.

"This is one of many, many campaigns that happen all the time and never make it into the public domain," said Alexander Klimburg, a cyber security expert at the Austrian Institute for International Affairs.



A computer engineer checks equipment at an internet service provider in Tehran on Feb. 15, 2011.

A cyber security agency in Iran said on its English website that Flame bore a "close relation" to Stuxnet, the notorious computer worm that attacked that country's nuclear program in 2010 and is the first publicly known example of a cyber weapon.

Iran's National Computer Emergency Response Team also said Flame might be linked to recent cyber attacks that officials in Tehran have said were responsible for massive data losses on some Iranian computer systems.

Kaspersky Lab said it discovered Flame after a U.N.

telecommunications agency asked it to analyze data on malicious software across the Middle East in search of the data-wiping virus reported by Iran.

### Stuxnet connection

Experts at Kaspersky Lab and Hungary's Laboratory of Cryptography and System Security who have spent weeks studying Flame said they have yet to find any evidence that it can attack infrastructure, delete data or inflict other physical damage.

Yet they said they are in the early stages of their investigations and that they may discover other purposes beyond data theft. It took researchers months to determine the key mysteries behind Stuxnet, including the purpose of modules used to attack a uranium enrichment facility at Natanz, Iran.

"Their initial research suggest that this was probably written by the authors of Stuxnet for covert intelligence collection," said John Bumgarner, a cyber warfare expert with the non-profit U.S. Cyber Consequences Unit think tank.

Flame appears poised to go down in history as the third major cyber weapon uncovered after Stuxnet and its data-stealing cousin Duqu, named after the Star Wars villain.

The Moscow-based company is controlled by Russian malware researcher Eugene Kaspersky. It gained notoriety after solving several mysteries surrounding Stuxnet and Duqu.

Their research shows the largest number of infected machines are in Iran, followed by Israel and the Palestinian territories, then Sudan and Syria.

The virus contains about 20 times as much code as Stuxnet, which caused centrifuges to fail at the Iranian enrichment facility it attacked.

It has about 100 times as much code as a typical virus designed to steal financial information, said Kaspersky Lab senior researcher Roel Schouwenberg.

### Gathering data

**Flame can gather data files, remotely change settings on computers, turn on PC microphones to record conversations, take screen shots and log instant messaging chats.**

Kaspersky Lab said Flame and Stuxnet appear to infect machines by exploiting the same flaw in the Windows operating system and that both viruses employ a similar way of spreading.

That means the teams that built Stuxnet and Duqu might have had access to the same technology as the team that built Flame, Schouwenberg said.

He said that a nation state would have the capability to build such a sophisticated tool, but declined to comment on which countries might do so.

The question of who built flame is sure to become a hot topic in the security community as well as the diplomatic world.

There is some controversy over who was behind Stuxnet and Duqu. Some experts suspect the United States and Israel, a view that was laid out in a January 2011 New York Times report that said it came from a joint program begun around 2004 to undermine what they say are Iran's efforts to build a bomb.

The U.S. Defense Department, CIA, State Department, National Security Agency, and U.S. Cyber Command declined to comment.

Hungarian researcher Boldizsar Bencsath, whose Laboratory of Cryptography and Systems Security first discovered Duqu, said his analysis shows that Flame may have been active for at least five years and perhaps eight years or more.

That implies it was active long before Stuxnet.

"It's huge and overly complex, which makes me think it's a first-generation data gathering tool," said Neil Fisher, vice president for global security solutions at Unisys Corp. "We are going to find more of these things over time."

Others said that cyber weapons technology has inevitably advanced since Flame was built.

"The scary thing for me is: if this is what they were capable of five years ago, I can only think what they are developing now," Mohan Koo, managing director of British-based Dtex Systems cyber security company.

Some experts speculated that the discovery of the virus may have dealt a psychological blow to its victims, on top of whatever damage Flame may have already inflicted to their computers.

"If a government initiated the attack it might not care that the attack was discovered," said Klimburg of the Austrian Institute for International Affairs. "The psychological effect of the penetration could be nearly as profitable as the intelligence gathered."

## Be afraid: Die Hard 4 reveals a real threat

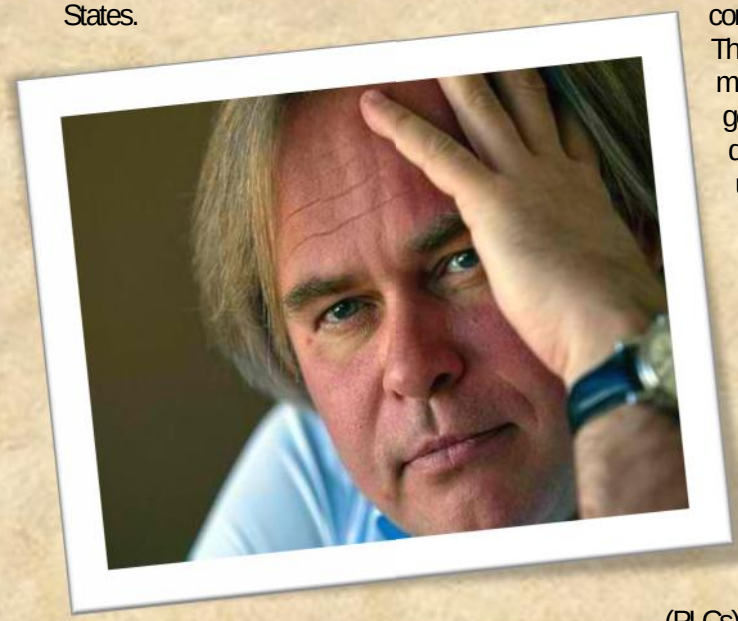
**Source:** http://www.smh.com.au/it-pro/security-it/be-afraid--die-hard-4-reveals-a-real-threat-20120528-1zeg0.html?goback=.gde_2708813_member_119700532

Five years on, John McClane's security nightmare is not so sci-fi.

Diligence and gritty determination may have helped Eugene Kaspersky become one of the software world's most successful entrepreneurs, but there's one thing the antivirus king can't bear: *Die Hard 4.0*.

"I watched the movie for 20 minutes, then pressed pause, got a cigarette and a glass of Scotch. To me it was really scary: they were talking about real scenarios. It was like a user guide for cyber terrorists. I hated that movie," the flamboyant Russian entrepreneur says.

The popular 2007 action film pits Bruce Willis' character, John McClane, against a domestic terrorist who's bent on launching a large-scale cyber attack that would disable financial markets, traffic lights, and other computer-controlled infrastructure across the United States.



Eugene Kaspersky, CEO of Kaspersky Labs, saw cyber threats coming. *Photo: Lee Besford*

For most viewers, it was nothing more than a fast-paced popcorn flick combining macho bravura with implausible technobabble. For Kaspersky it represented the popularisation of a relatively new mode of cyber attack that has now emerged as a real threat.

"We came to the [potential] of cyber terrorist attacks years before *Die Hard 4.0*," explains Kaspersky, the co-founder and chief executive of security firm Kaspersky Labs. "But it was forbidden in my company to explain it to journalists, because I didn't want to open Pandora's Box. I didn't want to let people think that my business is the business of fear. And I didn't want the bad guys to learn from these ideas."

His "silence" wasn't enough: as at least one high-profile hacking attack has recently shown, industrial control systems – and, in particular, SCADA (Supervisory Control and Data Acquisition) systems used to monitor and manage physical plant processes - can be a target of interest for a number of attackers, from hackers to military operations.

Because of their mission-critical nature, SCADA systems traditionally run on separate data networks with no internet or intranet connectivity. However, some have been brought online, to enable remote access and control.

Their security environments are often managed separately to those of the general enterprise, and they often run on different operating systems that aren't updated as often as enterprise software, leading some experts to believe SCADA systems present potential holes in the cyber defences of critical infrastructure operations.

The threat became clear in mid 2010 as the notorious Stuxnet worm spread across Windows desktops inside Iran's nuclear facilities, until it found systems running Step-7. The software application from German giant Siemens manages SCADA programmable logic controllers (PLCs) that control industrial process lines. It is believed Stuxnet then grant itself root access and reconfigured SCADA systems that met certain specific criteria.

An incident in 2000 brought SCADA sabotage to our shores as Queensland-based former Maroochy Shire Council (now Sunshine Coast Council) was forced to deal with attacks from disgruntled SCADA contractor Vitek Boden, whose work with a laptop and radio transmitter flooded parks, rivers, and a local hotel with 800,000 litres of raw sewage.

While isolated, these events remain a threat, says Bill Holder, a SCADA security expert.


"The threat from hackers is real," he explains, arguing that infrastructure authorities should build security controls at every level of the infrastructure to limit their exposure to major attacks.

"Catastrophic failure is one end of the scale, and is the type of thing that fail-safe [measures] and monitoring would mitigate. The idea of security is that it is not added on after everything else is done; it should be part of the overall design and development," Holder says.

"There has been a limited focus on security when it comes to control systems. Some of the control systems in place today are very old, and were installed long before security was an issue. In a perfect world with unlimited time and budgets it would be great to start again, but the reality is that a lot of money has been invested in control systems that can't just be thrown away."

Kaspersky is one of a large chorus of voices arguing for infrastructure operators to tighten SCADA security as a matter of priority – but even he admits that the high cost and long timeframe for replacing systems makes it unlikely much will change in the short term.

Holder agrees: "There is no reason to throw out perfectly good control system infrastructure if it can be made secure," he says. "The real key is whether the equipment can be brought up to standard."

Ongoing delays could leave any infrastructure operator exposed – with disastrous side effects if state-sponsored cyber attacks lead to all out cyberwar. Some consider Stuxnet to be the first volley in a new kind of economic and political conflict.

Many governments have moved to contain the possibility of unchecked cyber warfare, with the US and China recently running 'war games' testing cyber attacks.

Far from the rarefied heights of international cyber warfare, however, Kaspersky warns that companies can't be complacent when it comes to cyber-security. While new tools are constantly being developed and improved in an effort to keep up with often bloody-minded hackers, he believes companies need to make security an endemic part of their culture.

This includes everything from reworking long-unimproved administrative systems, to forcing senior business managers to undergo formal security training and certification. "These targeted attacks just started to happen on a regular basis in the last two years," he says. "Some of these incidents smell so high-level that I'm sure the bad guys were testing them before they attacked."

"Companies are becoming aware of this," he adds, "but it can take years to develop a new design. In the meantime, they should consider disconnecting some parts of the IT from the network; introducing military security standards to the enterprise environment; and making top managers pass security training. There is no 100 per cent security."

## Obama Order Sped Up Wave of Cyberattacks Against Iran

Source: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&pagewanted=1&pagewanted=all

From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Iran's nuclear enrichment facility at Natanz.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

Told it was unclear how much the Iranians knew about the code, and offered evidence that it was still causing havoc, Mr. Obama decided that the cyberattacks should proceed.

In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.

This account of the American and Israeli effort to undermine the Iranian nuclear program is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts. None would allow their names to be used because the effort remains highly classified, and parts of it continue to this day.

These officials gave differing assessments of how successful the sabotage program was in slowing Iran's progress toward developing the ability to build nuclear weapons. Internal Obama administration estimates say the effort was set back by 18 months to two years, but some experts inside and outside the government are more skeptical, noting that Iran's enrichment levels have steadily recovered, giving the country enough fuel today for five or more weapons, with additional enrichment.

Whether Iran is still trying to design and build a weapon is in dispute. The most recent United States intelligence estimate concludes that Iran suspended major parts of its weaponization effort after 2003, though there is evidence that some remnants of it continue.

Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the

head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare." But there has been scant evidence that it has begun to strike back.

The United States government only recently acknowledged developing cyberweapons, and it has never admitted using them. There have been reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year. But Olympic Games was of an entirely different type and sophistication.

It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University in April. Those forensic investigations into the inner workings of the code, while picking apart how it worked, came to no conclusions about who was responsible.

A similar process is now under way to figure out the origins of another cyberweapon called Flame that was recently discovered to have attacked the computers of Iranian officials, sweeping up information from those machines. But the computer code appears to be at least five years old, and American officials say that it was not part of Olympic Games. They have declined to say whether the United States was responsible for the Flame attack.

Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.

"We discussed the irony, more than once," one of his aides said. Another said that the administration was resistant to developing a "grand theory for a weapon whose possibilities they were still discovering." Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.

### A Bush Initiative

The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America's European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation's nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before.

Iran's president, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described grand ambitions to install upward of 50,000 centrifuges. For a country with only one nuclear power reactor — whose fuel comes from Russia — to say that it needed fuel for its civilian nuclear program seemed dubious to Bush administration officials. They feared that the fuel could be used in another way besides providing power: to create a stockpile that could later be enriched to bomb-grade material if the Iranians made a political decision to do so.

Hawks in the Bush administration like Vice President Dick Cheney urged Mr. Bush to consider a military strike against the Iranian nuclear facilities before they could produce fuel suitable for a weapon. Several times, the administration reviewed military options and concluded that they would only further inflame a region already at war, and would have uncertain results.

For years the C.I.A. had introduced faulty parts and designs into Iran's systems — even tinkering with

imported power supplies so that they would blow up — but the sabotage had had relatively little effect. General James E. Cartwright, who had established a small cyberoperation inside the United States Strategic Command, which is responsible for many of America's nuclear forces, joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.


The goal was to gain access to the Natanz plant's industrial computer controls. That required leaping the electronic moat that cut the Natanz plant off from the Internet — called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialized computers that command the centrifuges.

The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. The connections were complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail.

Eventually the beacon would have to "phone home" — literally send a message back to the headquarters of the National Security Agency that would describe the structure and daily rhythms of the enrichment plant. Expectations for the plan were low, one participant said the goal was simply to "throw a little sand in the gears" and buy some time. Mr. Bush was skeptical, but lacking other options, he authorized the effort.

### Breakthrough, Aided by Israel

It took months for the beacons to do their work and report home, complete with maps of the electronic directories of the controllers and what amounted to blueprints of how they were connected to the centrifuges deep underground.

Then the N.S.A. and a secret Israeli unit respected by American intelligence officials for its cyberskills set to work developing the enormously complex computer worm that would become the attacker from within.

The unusually tight collaboration with Israel was driven by two imperatives. Israel's Unit 8200, a part of its military, had technical expertise that rivaled the N.S.A.'s, and the Israelis had deep intelligence about operations at Natanz that would be vital to making the cyberattack a success. But American officials had another interest, to dissuade the Israelis from carrying out their own pre-emptive strike against the Iranian nuclear facilities. To do that, the Israelis would have to be convinced that the new line of attack was working. The only way to convince them, several officials said in interviews, was to have them deeply involved in every aspect of the program.

Soon the two countries had developed a complex worm that the Americans called "the bug." But the bug needed to be tested. So, under enormous secrecy, the United States began building replicas of Iran's P-1 centrifuges, an aging, unreliable design that Iran purchased from Abdul Qadeer Khan, the Pakistani nuclear chief who had begun selling fuel-making technology on the black market. Fortunately for the United States, it already owned some P-1s, thanks to the Libyan dictator, Col. Muammar el-Qaddafi.

When Colonel Qaddafi gave up his nuclear weapons program in 2003, he turned over the centrifuges he had bought from the Pakistani nuclear ring, and they were placed in storage at a weapons laboratory in Tennessee. The military and intelligence officials overseeing Olympic Games borrowed some for what they termed "destructive testing," essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department's national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.

Those first small-scale tests were surprisingly successful: the bug invaded the computers, lurking for days or weeks, before sending instructions to speed them up or slow them down so suddenly that their delicate parts, spinning at supersonic speeds, self-destructed.
After several false starts, it worked. One day, toward the end of Mr. Bush's term, the rubble of a centrifuge was spread out on the conference table in the Situation Room, proof of the potential power of a cyberweapon. The worm was declared ready to test against the real target: Iran's underground enrichment plant.
"Previous cyberattacks had effects limited to other computers," Michael V. Hayden, the former chief of the C.I.A., said, declining to describe what he knew of these attacks when he was in office. "This is the first attack of a major nature in which a cyberattack was used to effect physical destruction," rather than just slow another computer, or hack into it to steal data.
"Somebody crossed the Rubicon," he said.
Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others — both spies and unwitting accomplices — with physical access to the plant. "That was our holy grail," one of the architects of the plan said. "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."
In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.
The first attacks were small, and when the centrifuges began spinning out of control in 2008, the Iranians were mystified about the cause, according to intercepts that the United States later picked up. "The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence," one of the architects of the early attack said.
The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. "This may have been the most brilliant part of the code," one American official said.
Later, word circulated through the International Atomic Energy Agency, the Vienna-based nuclear watchdog, that the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw.
"The intent was that the failures should make them feel they were stupid, which is what happened," the participant in the attacks said.
When a few centrifuges failed, the Iranians would close down whole "stands" that linked 164 machines, looking for signs of sabotage in all of them. "They overreacted," one official said. "We soon discovered they fired people."
Imagery recovered by nuclear inspectors from cameras at Natanz — which the nuclear agency uses to keep track of what happens between visits — showed the results. There was some evidence of wreckage, but it was clear that the Iranians had also carted away centrifuges that had previously appeared to be working well.
But by the time Mr. Bush left office, no wholesale destruction had been accomplished.
Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush's advice.

### The Stuxnet Surprise

Mr. Obama came to office with an interest in cyberissues, but he had discussed them during the campaign mostly in terms of threats to personal privacy and the risks to infrastructure like the electrical grid and the air traffic control system. He commissioned a major study on how to improve America's defenses and announced it with great fanfare in the East Room.
What he did not say then was that he was also learning the arts of cyberwar. The architects of Olympic Games would meet him in the Situation Room, often with what they called the "horse blanket," a giant foldout schematic diagram of Iran's nuclear production facilities.
Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously.
"From his first days in office, he was deep into every step in slowing the Iranian program — the diplomacy, the

sanctions, every major decision," a senior administration official said. "And it's safe to say that whatever other activity might have been under way was no exception to that rule."

But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.

An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.

"We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know if we were part of that activity."

Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. "It's got to be the Israelis," he said. "They went too far."

In fact, both the Israelis and the Americans had been aiming for a particular part of the centrifuge plant, a critical area whose loss, they had concluded, would set the Iranians back considerably. It is unclear who introduced the programming error.

The question facing Mr. Obama was whether the rest of Olympic Games was in jeopardy, now that a variant of the bug was replicating itself "in the wild," where computer security experts can dissect it and figure out its purpose.

"I don't think we have enough information," Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran's oil revenues.

Within a week, another version of the bug brought down just under 1,000 centrifuges. Olympic Games was still on.

### A Weapon's Uncertain Future

American cyberattacks are not limited to Iran, but the focus of attention, as one administration official put it, "has been overwhelmingly on one country." There is no reason to believe that will remain the case for long. Some officials question why the same techniques have not been used more aggressively against North Korea. Others see chances to disrupt Chinese military plans, forces in Syria on the way to suppress the uprising there, and Qaeda operations around the world. "We've considered a lot more attacks than we have gone ahead with," one former intelligence official said.

Mr. Obama has repeatedly told his aides that there are risks to using — and particularly to overusing — the weapon. In fact, no country's infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran.

*This article is adapted from "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," to be published by Crown on Tuesday (June 3, 2012).*

## India: Cyber Terrorism And The Fifth Domain – Analysis

**By Sanchita Bhattacharya**

Source: http://www.eurasiareview.com/05062012-india-cyber-terrorism-and-the-fifth-domain-analysis/

Expressing grave concern about the growing threat of cyber terrorism in his opening statement at the meeting of Chief Ministers on National Counter Terrorism Centre (NCTC) held on May 5, 2012, Union

Home Minister P. Chidambaram stated:
*…there are terrorist threats in the cyber space, which is the fifth domain after land, sea, air and space. Much of our critical infrastructure lies in cyber space. Cyber crimes such as hacking, financial fraud, data theft, espionage etc. would, in certain circumstances, amount to terrorist acts. Our counter terrorism (CT) capacity must be able to meet the threats in cyber space. Since there are no boundaries in cyber space, how will the Central Government and the State Governments share the responsibility to face the threats in cyber space?*

## India

Chidambaram was, of course, using the cyber threat to buttress his arguments in favour of the NCTC, a pet project that has met with tremendous resistance from the States. Nevertheless, the threat of cyber terrorism is real and growing, as global and national systems become increasingly interlinked and interdependent. Indeed, speculation about the potential threat of cyber attacks has been rife since the 1980s, and Government systems across the world have been targeted from time to time, principally in marginally disruptive and vandalizing actions, variously, by politically motivated, mischievous and state backed groupings. Definitional disputes abound, and it is not clear how many of these can be described as cyber terrorist 'attacks'. Nevertheless, cyber technology has become a crucial tool in the terrorist arsenal, and its use to directly engineer widespread, and potentially life threatening, disruptions cannot be overestimated. The US Government's Stuxnet attack against Iran's principal uranium enrichment facilities, which experts believe may stall Iran's nuclear program by as much as five years, recently demonstrated the potential capability of cyber war interventions.

Cyber technology has played a role – albeit principally as a covert communication, propaganda or psychological warfare tool – in terrorist activities in India, for some time now. This includes prominent attacks in cities including Ahmedabad, Jaipur, Delhi, Mumbai and Varanasi, among others, over the past years. Significantly, the perpetrators of the November 26, 2008, Mumbai terrorist attacks (26/11), which claimed 166 lives, made substantial use of cyber technology in preparing and mounting the operation. US Marine Corps Lieutenant General George J. Flynn, on May 15, 2012, observed, "All the (26/11) mission planning was done via Google Earth… The terrorists used cellular phone networks as command and control and social media to track and thwart the efforts of Indian commandos." He noted, further, "Space and cyber will continue to play an increased role in events, with each becoming increasingly contested domains – so it's a new domain that we're going to have to contest."

A December 2008 report had earlier noted that the Pakistan-backed Lashkar-e-Toiba (LeT) had used Voice-over Internet Protocol (VoIP) software to communicate with the 26/11 attackers on the ground and direct the large scale operation on a real-time basis. Citing Indian intelligence sources, the report claimed that the attackers' handlers "were apparently watching the attacks unfold live on television [and] were able to inform the attackers of the movement of security forces from news accounts and provide the gunmen with instructions and encouragement". The distinguishing feature of VoIP-based communications, which form the technical basis of popular communications software such as Skype and Vonage, is that audio signals are converted to data and travel through most of the Internet infrastructure in binary, rather than audio, format, making them near impossible to detect and proactively intercept.

After the terrorist attack on Delhi High Court on September 7, 2011, in which 15 persons were killed and another 87 were injured, investigative assistance was sought from the US and some south-east Asian countries, including Myanmar, Thailand, Malaysia and Indonesia, to trace back cyber linkages connected with the incident. Terrorists had hacked into

unsecured wi-fi internet connections to send e-mails after the attack.

The Indian Mujahedeen (IM) has carried out over a dozen high profile attacks, including the May 13, 2008, Jaipur (Rajasthan) bombings; the July 25, 2008, Bangalore (Karnataka) serial blasts; the July 26, 2008, Ahmedabad (Gujarat) serial blasts; the September 13, 2008, Delhi serial blasts; the Pune German Bakery blasts of February 13, 2010; and the Mumbai serial blasts of July 13, 2011. Before almost all of these attacks, IM activists sent out e-mails to various media organisations.

Police traced e-mails sent by IM from Navin Computer in Sahibabad area of Ghaziabad District in Uttar Pradesh (UP) soon after the May 13, 2008, Jaipur (Rajasthan) blast, which claimed 80 lives. Three video clips attached to one of the e-mails showed two explosive-fitted bicycles moments before they were detonated. The e-mails were sent from two accounts – guru_al_hindi_jaipur@yahoo.co.uk and guru_al_hindi@yahoo.fr.

IM activists had hacked into the unsecured wi-fi internet connection of an American national, Kenneth Haywood, residing in the Sanpada area of Navi Mumbai, minutes before the July 26, 2008, Ahmedabad terror attack, which killed 53 people. An e-mail claiming the attack was sent prior to the blasts from his Internet Protocol (IP) address.

After the September 19, 2010, Jama Masjid (Delhi) attack, Delhi Police confirmed, a day later, that the IM had sent a threat e-mail from the IP address of a computer in Mumbai.

Investigations into the Varanasi (UP) blast of December 7, 2010, highlighted the need for 'wardriving' to detect threat mails posted by IM, allegedly from Mumbai. 'Wardriving' is used to search for wi-fi wireless networks with the help of a laptop from a moving vehicle, in order to detect unsecured wi-fi internet points that may be exploited.

The LeT has attained a significant degree of 'cyber efficiency', and has been making increasing use of VoIP for communications. LeT's 26/11 'master-mind', Zaki-ur Rehman Lakhvi, who is presently in a Rawalpindi (Pakistan) jail, is known to have been networking with LeT cadres from jail, using a private VoIP on his smart phone. "Lakhvi's compound serves as Lashkar's alternative headquarters," an unnamed top intelligence source disclosed. Pakistan-based LeT, which is headed by Hafiz Mohammad Saeed, started using VoIP as soon as the technology became common in the early 2000s. Highlighting the problems this creates, an unnamed intelligence source explained, "Earlier, we could intercept conversations on phone or locate Lashkar cadres based on their IP addresses through their emails. But now we're finding it tough to gather intelligence because Lashkar men hold audio or video conferences using private VoIP".

According to an article written by Ravi Visvesvaraya Prasad, published in The Hindustan Times on December 19, 2000, a number of Pakistani hacker groups, including 'Death to India', 'Kill India', and 'G-Force Pakistan', have openly circulated instructions for attacking Indian computers. Websites run by Nicholas Culshaw of Karachi, and another run by Arshad Qureshi of Long Beach, California, circulated malicious anti-Indian propaganda along with step-by-step instructions for hacking into thousands of Indian websites. Anti-Indian terrorist instructions were also hosted by http://62.236.92.165, http://209.204.7.131, and http://209.204.5.113. All these sites appear to be disabled now, but their architects quickly recreate new platforms.

On December 3, 2010, in a breach of security was detected on the Central Bureau of Investigation (CBI) website, which had been hacked by the 'Pakistan Cyber Army'. The CBI home page carried a message from the 'Pakistani Cyber Army' warning India not to attempt to attack their websites. It further claimed to have defaced another 270 Indian websites.

Interestingly, according to the report of the Security and Defence Agenda (SDA), a leading defence and security think-tank in Brussels (Belgium) and McAfee, India has been ranked fifth in the worldwide ranking of countries affected by Cyber Crime.

Explaining the severity of Cyber Crime in India, Minister of State for Communications and Information Technology, Sachin Pilot, on March 26, 2012, informed the Rajya Sabha (Upper House of Parliament) that cyber crimes were on the rise in the country. He also palced data maintained by the National Crime Records Bureau (NCRB) before Parliament, documenting the number of cyber crime cases and related arrests under the Information Technology Act, 2000:

| Years | Cyber Crime Cases | Arrests |
|---|---|---|
| 2007 | 217 | 154 |
| 2008 | 288 | 178 |
| 2009 | 420 | 288 |
| 2010 | 966 | **799** |

Further, the number of cases registered under Cyber Crime related sections of Indian Penal Code (IPC), along with the number of arrests, were given as:

| Years | Cyber Crime Cases | Arrests |
|---|---|---|
| 2007 | 328 | 429 |
| 2008 | 176 | 195 |
| 2009 | 276 | 263 |
| 2010 | 356 | **294** |

Earlier, explaining the threat faced by Government websites due to Cyber Crime in the Lok Sabha (Lower House of Parliament), the Minister had stated, on November 30, 2011, that a total of 90, 119, 252 and 219 Government websites, as reported and tracked by the Indian Computer Emergency Response Team (CERT-In), had been defaced by various hacker groups in the year 2008, 2009, 2010 and January–October 2011, respectively.

As far Government initiative is concerned, following the 26/11 attacks, the Information Technology Act, 2000, has been amended by Information Technology (Amendment) Act, 2008 with effect from October 27, 2009. The amended Act is a comprehensive Act and provides legal framework to fight all prevalent cyber crimes. Stringent punishment ranging from imprisonment of three years to life imprisonment and fine has been provided for various acts of cyber crime.

On March 27, 2012, explaining Government initiatives to contain Cyber Crime, Pilot informed the Rajya Sabha that a major programme had been initiated on the development of cyber forensics, setting up of infrastructure for investigation and training of users, including Police and judicial officers, and training for the collection and analysis of digital evidence. He disclosed that the Data Security Council of India (DSCI) had organized 112 training programmes on Cyber Crime Investigation and awareness, and a total of 3,680 Police and judicial officers, as well as public prosecutors, had been trained.

On May 16, 2012, National Security Advisor Shiv Shankar Menon disclosed that the Government was in the 'final stages' of preparing the 'national cyber security architecture' and would hold consultations on the subject with the National Association of Software and Services Companies (NASSCOM), the apex body of the software and services companies in India, in June.

Cyber crimes and the use of cyber space and technologies by terrorists are, currently, at worst, powerful facilitators for terrorist groups. In the main, they remain marginal irritants to the system. Nevertheless, the potential threat they constitute is grave, and this has been noticed by the Indian state. A decision has been taken to establish a National Cyber Coordination Centre, a full-fledged agency to counter this menace. However, current deficits in trained manpower and state of art equipment and infrastructure may hobble effective operationalization for some time. A race is currently on, with terrorists, on the one hand, pushing the frontiers of cyber space to harness the most disruptive of tools possible, and state agencies, on the other, seeking to interdict them in this enterprise. It remains to be seen which side in the conflict has the greater coherence and more sustained motivation.

***Sanchita Bhattacharya*** *is a Research Assistant, Institute for Conflict Management*

## Cyberweapons: Bold steps in a digital darkness?

Source: http://thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness

In 1945, the United States organized a committee to investigate whether nuclear weapons should become a central military technology, or whether to abjure the weapons and, through self-restraint, avoid a costly and potentially deadly nuclear arms race. Led by Undersecretary of State Dean Acheson and Chairman of the Tennessee Valley Authority David Lilienthal, the committee produced the eponymous Acheson-Lilienthal Report, which, after it failed to gather reasonable support, marked

a turning point in the Cold War and signaled the beginning of the nuclear arms race. Almost 70 years later, we find ourselves at a similar juncture with cyberwarfare. Cyber weapons do not appear to be capable of mass destruction in the way nuclear weapons clearly are, but they hold at risk some of the most precious assets of our time: the information storage and control mechanisms on which
modern society has been built. It is not difficult to imagine catastrophic scenarios such as the destruction of a banking sector, the elimination of a stock market, the flooding of a dam, or the poisoning of a water supply -- all initiated by malfunctions induced by malicious software. The United States rushed into the nuclear age eager to cement its technical superiority, causing a decades-long nuclear arms race that threatened global extinction. Before policymakers go too far, they should now take a moment to consider the implications -- both intended and unintended -- of cyberweapons.

While digital spying has taken place for decades, the era of computer-mediated destruction has only recently begun. Early this month *The New York Times* published an investigative feature that explored Olympic Games, a cyberweapons program designed to sabotage an element of another country's infrastructure. Started during the Bush administration, this is the first known program of its kind. In embarking on Olympic Games, the United States and Israel stepped boldly, but naively, into uncharted territory.

The first battle of Olympic Games reached the public eye in July 2010, when news broke of Stuxnet, a creative worm designed to cause Iran's uranium-enrichment centrifuges to explode by changing, with software, their operating parameters. On its heels were Duqu, Wiper, and Flame, a set of multipurpose tools that collected intelligence, identified vulnerabilities, and sabotaged information systems.

In some small way, the strategic vision of Olympic Games is commendable. Cyberattacks might have reduced Israeli pressure for conventional military strikes that could have led to a deadly and protracted war with Iran and triggered Iran to race for the bomb. The cyberstrategy might have also been rationalized as providing more opportunity for diplomacy -- but as with most experimental programs, events did not go according to plan and unforeseen consequences soon emerged.

Consider as a case study Stuxnet: First injected into Iran's computers in June 2009, the worm appears to have destroyed more than 1,000 of Iran's 5,000 gas centrifuges, according to data reported by the International Atomic Energy Agency (IAEA). However, by drawing from its centrifuge reserves, Iran was able to replace quickly its destroyed centrifuges and compensate for the losses, even while the Stuxnet attack was ongoing.

Indeed, if the measure of Iran's progress toward a nuclear weapon is its inventory of enriched uranium, then Iran came out ahead. IAEA data indicates that Iran was able to boost output enough to reverse all Stuxnet-induced production losses by March 2010, about eight months after the attack first began to have an effect. After the successful eradication of Stuxnet in the summer of 2010, Iran sustained its heightened level of production, expanding its low-enriched uranium stockpile at rates exceeding the pre-Stuxnet trend. If, without Stuxnet, Iran would have expanded production according to its historical trajectory, then one would conclude that the cyberattack wound up enhancing Iran's ability to make nuclear weapons instead of setting the program back.

What went wrong? Stuxnet was designed to operate on an ongoing basis without being detected: a strategy of steady attrition in the pursuit of time. The worm was not supposed to leave Iran or be discovered -- but it soon spread beyond the confines of Iran's nuclear

***Article Highlights***

- The United States rushed into the nuclear age eager to cement its technical superiority, disregarding warnings of key statesmen and scientists that a decades-long nuclear arms race would ensue. Before they go too far, policymakers should consider the implications -- both intended and unintended -- of cyberweapons.
- Though Israel and the United States may have vast resources to support sophisticated and creative cyberweapons programs, it is worth remembering that such advantage could be its disadvantage: Each new cyberattack becomes a template for other nations -- or sub-national actors -- looking for ideas.
- As nations begin to develop cyberwarfare organizations, they run the risk of creating bureaucratic entities, which will protect offensive cyber capabilities that simultaneously subject their own publics to cyber vulnerabilities. Since the United States has the most to lose in this area, the safe approach is to direct cyber research at purely defensive applications.

facilities until, ultimately, members of the computer-security community identified PDF it. Stuxnet both failed to operate according to plan and failed to have a long-term benefit. Perhaps, then, the lesson for the authors of future cyberweapons is to recognize the short-lived and unpredictable nature of cyberattacks and aim for more acute, immediate destruction, rather than persistent manipulation of another nation's assets -- a worrisome conclusion suggesting that cyberweapons may be better suited for terror than for strategic affairs.

After Stuxnet, other components of the cyber affront were quickly exposed and removed, and Iran's uranium-enrichment capabilities grew faster than ever. The American and Israeli leaders who launched the games suddenly found themselves in a state of panic. Their ability to influence Iran's nuclear program had dropped precipitously, yet no diplomatic progress had been made to ensure a soft landing. Perhaps leaders had grown too narrowly focused on the play-by-play excitement of a new cyberattack and too comfortable with relative inaction on the diplomatic front. Or perhaps leaders began to feel that a technical fix was potentially within reach, or at least that cyberattacks could hold Iran's nuclear program at bay until its leaders capitulated to the pressure of sanctions. Whatever the likely reasons, the current reality is that the United States finds the diplomatic challenge harder than ever before: After Stuxnet, Iran, with even larger centrifuge reserves, has more to sacrifice, but now trusts the United States even less. Furthermore, Israeli threats of armed conflict have reached a new high. The situation has become unstable, and Olympic Games has yet to realize any enduring benefits.

Despite their questionable utility, the cyberattacks have not been without consequence. Immediately after Iran admitted to being a victim of Stuxnet, it created a new Cyber Command of its own. Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare," a formula that may imply aspirations to go on the offensive. The US Defense Department responded by announcing a new policy in which cyberattacks against US assets are considered to be acts of war. More bold steps into the darkness.

In the world of armaments, cyber weapons may require the fewest national resources to build. That is not to say that highly developed nations are not without their advantages during early stages. Countries like Israel and the United States may have more money and more talented hackers. Their software engineers may be more skilled and exhibit more creativity and critical thinking owing to better training and education. However, each new cyberattack becomes a template for other nations -- or sub-national actors -- looking for ideas. Stuxnet revealed numerous clever solutions that are now part of a standard playbook. A Stuxnet-like attack can now be replicated by merely competent programmers, instead of requiring innovative hacker elites. It is as if with every bomb dropped, the blueprints for how to make it immediately follow. In time, the strategic advantage will slowly fade and once-esoteric cyber weapons will slowly become weapons of the weak.

Whatever the greater nature of cyberwarfare, it is clear that individual cyberweapons are inherently fragile. They work because they exploit previously unknown vulnerabilities. Stuxnet, for example, exploited four "zero day" vulnerabilities in the Windows operating system. As soon as Stuxnet made them public, they were patched and thus no longer available vectors for future attacks or intelligence gathering. Such vulnerabilities are also closed through routine software updates and patches. Powerful hacker entities like the US National Security Agency must continue to discover new weaknesses in an attempt to stay ahead, and probably maintain a sizable list of unpublished vulnerabilities for future exploitation -- but to what end? These security gaps apply to all computer systems of a specific type regardless of national borders. Every vulnerability kept secret for the purpose of enabling a future cyberattack is also a decision to let that vulnerability remain open in one's own national infrastructure, allowing it to be exploited by an enemy state or even a terrorist hacker. This raises a basic philosophical question about how states should approach the question of cyberwarfare: Should countries try to accrue offensive capabilities in what amounts to a secret arms race and, in doing so, hold their own publics at risk? Or should states take a different tack, releasing knowledge about vulnerabilities in a controlled way to create patches to

shore up their own digital frontiers?

We are at a key turning point -- the Acheson and Lilienthal moment of the digital age in which a nation must decide what role cyberweapons will play in its national defense. As nations begin to build out cyberwarfare organizations, they run the risk of creating bureaucratic entities that will seek to protect offensive cyber capabilities and in doing so will necessarily subject their own publics to cyber vulnerabilities. For states that have little to lose on the cyber front, an offensive approach may be interesting. But for the United States and other highly developed nations whose societies are critically and deeply reliant on computers, the safe approach is to direct cyber research at purely defensive applications. Fortunately, unlike the Acheson and Lilienthal moment of the nuclear age, the United States can make this choice unilaterally. The alternative approach, to continue to launch ambitious cyberattacks, is to cross the Rubicon with an unpracticed weapon, naked to the attacks of enemies and terrorists alike.