Towards a Chemical War in Syria ?

CBRNE Newsletter Terrorism

Volume 46, 2012

Cyber News

Happy New Year

2013

www.cbrne-terrorism-newsletter.com

Concentrate on cyber attacks, not terrorism

Source: http://www.telegraph.co.uk/technology/internet-security/9637186/Concentrate-on-cyber-attacks-not-terrorism-Osborne-tells-spy-chiefs.html

British intelligence agencies' counter-terrorism work could be scaled back after an intervention from George Osborne.

However, senior ministers and officials are resisting pressure from the Treasury, warning that cutting counter-terrorism spending is too much of a risk.

MI6, the Secret Intelligence Service, is said to be fighting a fierce rearguard action against any move to reallocate its counter-terrorism resources. Theresa May, the Home Secretary, is also said to be cautious about relaxing Britain's defences against extremist attacks.

Senior sources have disclosed that Mr Osborne has asked agency chiefs if, following the London Olympics, Britain's spending on intelligence should be shifted significantly away from counter-terrorism. The Chancellor is understood to have asked them to consider how current spending decisions might look in the coming decades, suggesting future generations might question why today's leaders did not devote more resources to cyber security.

His intervention, at a meeting of the National Security Council in the summer, is understood to have inflamed a row within Whitehall about the intelligence agencies' future priorities. MI5, MI6 and GCHQ are all under growing pressure to do more to defend British interests from internet-based attacks.

The Intelligence and Security Committee of senior MPs and peers this year said it was "concerned that much of the work to protect UK interests in cyberspace is still at an early stage" and suggested the work should be stepped up urgently.

William Hague, the Foreign Secretary, this week told The Daily Telegraph that he saw evidence daily showing "deliberate, organised attacks" against corporate and government networks from "cyber criminals or foreign actors".

However, the agencies are said to be at odds over how much to spend on internet-based work, who should pay, and which agency should take the lead.

One Whitehall source described the situation as "a typical Whitehall turf-war", warning that the disputes could hamper the agencies' bid for funding in the next spending round. The combined budget for the intelligence agencies will be £2.1 billion in 2014-15, a cut of 7 per cent over four years.

Mr Osborne's challenge over terrorism is his second major intervention on security issues in recent months. Earlier this month, The Daily Telegraph disclosed that he had helped force military commanders to draw up plans for a faster British withdrawal from Afghanistan.

James Brokenshire, the security minister, declined to comment on discussions at the NSC, but said that intelligence officials "constantly examine" new and emerging threats to the UK.

He said: "Clearly, national security is the absolute priority for any government and therefore we will always ensure that national security receives sufficient funding.

"Does that mean that we shouldn't constantly innovate and look at ways in which we can be more effective? No, it does not. But clearly that underlying responsibility remains."

The New Reality of Cyber War

Contributor: James Farwell and Rafal Rohozinski
Source:http://www.defenceiq.com/cyber-defence/articles/the-new-reality-of-cyber-wa/&mac=DFIQ_OI_Featured_2011&utm_source=defenceiq.com&utm_medium=email&utm_campaign=DFIQOptIn&utm_content=10/31/12

The June 2012 report by New York Times chief Washington correspondent David Sanger that the Stuxnet cyber worm was only part of a broader operation, Olympic Games, launched against Iran by the United States and Israel affirmed what many suspected: cyber attack is not a distant theoretical probability. *(1)*

Stuxnet was the first alleged identified instance of weaponised computer code or malware employed as a 'use of force'. But it was not alone. Two other targeted computer viruses for espionage have surfaced: Duqu in September 2011, followed by Flame in May 2012. Media reports allege that both also targeted Iran.*(2)* As tools of espionage, use of neither would qualify as a use of force, but reflect new emphasis on cyber tools. Of the two, Flame drew wider attention. Apparently 20 times more complex than Stuxnet, Flame affected computers in Lebanon, the United Arab Emirates, the West Bank and Iran. It is said to have gathered intelligence by logging keyboard strokes, recording conversations by activating microphones, and taking screen shots. At Iran's oil ministry and oil-export terminal, the virus also erased information on hard discs while gathering information.*(3)* Many attribute it to the United States and Israel. These allegations remained unconfirmed by either government.

A new era

These developments put the spotlight on a new era of international engagement. Israeli sources have long boasted about Israel's involvement in Stuxnet. The US/Israeli use of Stuxnet as reported in detail by Sanger has arguably created a new de facto norm for the conduct of cyber engagements other nations can follow or imitate. Previously, a key constraint on the use of software as a weapon has been the potential for legal liability arising out of collateral damage inflicted upon innocent parties not targeted. In practice, software can be narrowly targeted to surmount that challenge.

What Stuxnet shows is that it is possible to have the specific intended effect while avoiding or minimising unplanned side effects by clearly differentiating between the propagator, or boost-phase code that disseminates the program, and the actual payload code that creates the physical effect on a target (the distinction between the gift wrapping and the gift). The reported operation did apparently limit the scope of damage. Stuxnet shows that one can surmount concerns that malware would take down the global network, not just a specific target. The lesson is that cyber weapons are in a different category from nuclear devices, which have little practical use except as a deterrent.

The rules of conduct for the use of code are evolving. As parties develop more sophisticated capabilities and acquire experience in their use, the picture will grow more complicated and nuanced. The strategic situation contains echoes of the period between the two world wars, when rapid developments in new technologies and domains of war-fighting preceded an understanding of how effectively to employ them operationally. Tanks changed the way armies engaged in battle. But despite British and German experimentation with armour in the inter-war period, armoured tactics could only be proven and fully developed on the battlefield from 1939 onwards. There are, moreover, significant differences of view about whether the Germans, renowned for their blitzkrieg tactics, properly understood the strategic use of armour for manoeuvre warfare.

Reports that two states have employed code against another state against which war has not been declared undercuts the common view that risks of escalation render state-to-state cyber war implausible. Sanger reported that President George W. Bush, under whom Olympic Games was apparently initiated, desired that use of Stuxnet not violate the rules of armed conflict.*(4)* The Law of Armed Conflict does not prohibit damage to such critical infrastructure. But a strength of using code is that the targeting process can manage the risks.

Stuxnet may appear as embryonic as the British Mk.1 tanks that made their debut at the Battle of the Somme in 1916. But technology moves quickly. Modern states rightly fear cyber war. Evolving technology is accelerating the flow of information, placing unique pressures on decision-making. Responding to cyber attack may require making decisions at network speed using systems that are themselves targeted. The potential for cascading effects is amplified by the interconnectedness of cyberspace. Stuxnet worked leisurely. Future combat in cyberspace may be more akin to the global trading system than existing forms of kinetic engagement, and present a different strategic calculus.

Active defence versus first strike

As described by Sanger, Olympic Games puts into question the existing discourse over US doctrines of active defence versus offensive use of malware and the strategic communication employed to explain US actions. Nations have been rightfully unwilling to disclose their doctrines for the offensive use of cyber weapons. Open-source discourse has centred on delineating passive and active defence. No nation has been willing to declare its intent to use cyber weapons offensively for a first strike. But Stuxnet blurs the lines between what might constitute active defence and offense. It also moves the impact from the strictly cyber realm to one that may entail mechanical or physical damage.

Passive cyber defence is easiest to grasp. The notion includes firewalls, cyber 'hygiene' that trains an educated workforce to guard against errors or transgressions that can lead to cyber intrusion,*(5)* detection technology, 'honey pots ' or decoys that serve as diversions, and managing cyberspace risk through collective defence, smart partnerships, information training, greater situation awareness, and establishing secure, resilient network environments.*(6)* Active cyber defence is a more elusive notion. Industry operates under different legal constraints than the military and they view the notion of active defence differently. For industry, the notion includes working actively with private-sector partners to identify and interdict cyber intrusions. Action beyond that raises real concerns. Under US law causing more than $5,000 of damage to another computer is a felony.*(7)* US anti-trust*(8)* and privacy laws*(9)* raise other concerns. Yet private industry owns and operates 90% of US civilian critical infrastructure. Its concerns will grow as future malware come into play, for

current laws and operational capabilities provide inadequate defences.

The public sector operates under different rules. While private parties can take action unless prohibited by law, the military can act only within its prescribed authority. As a result, the military's notion of active defence remains unformed: no one is certain what it means or how to apply it. The Pentagon has made clear it would employ force to defend against cyber attacks.*(10)* But who has the authority to launch what actions, and under what circumstances? If a hostile force targets a naval cruiser for imminent attack, does the captain hold the authority to launch a preemptive attack? If he doesn't, who does? Should he try to move his vessel out of danger? What if he cannot? How can he 'actively' mount a defence?

US Cyber Command Chief General Keith Alexander has declared that 'a Commander's right to self-defence is clearly established in both U.S. and international law'.*(11)* He did not define what that entails. Would it include hot pursuit? Former US Air Force Secretary Michael Wynne has stated that

US law allows 'hot pursuit' of criminals, enabling law enforcement to track and address cyber crime through the digital world.*(12)* That doctrine is well accepted in crime fighting,*(13)* but where it applies may hang on the status of an attacker. What rules govern may depend upon the status of an event as criminal activity, a military attack or a terrorist action.

Hot pursuit may well apply in cyberspace. Many concur that the law of the sea sanctions the use of the doctrine in the maritime domain,*(14)* which along with air, land, and space is viewed as a global commons. President Barack Obama has declared that cyberspace is also a 'recognized strategic commons'.*(15)*

A use of force?

For the most part the US discussion on cyber war has revolved around these notions of defence. But Olympic Games has apparently shown that the United States and Israel will use cyber weapons offensively.

The United States has previously said that its cyber strategies would respect international law. The key normative standards nest in United Nations Charter articles 2(4) and 51. Article 2(4) prohibits the 'threat or use of force against the territorial integrity or independence of any state'. Article 51 states that nothing 'in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations'.

But 'force' is not defined. There is no international convention that defines whether the use of software code should be deemed equivalent to the use of force. Cyber expert Herbert Lin has argued that the term almost certainly covers conventional-weapon attacks that injuring persons or irreparably damage property, but excludes economic or political acts (such as sanctions) that do not. In that view, Stuxnet would have constituted a use of force only if it had inflicted damage comparable to a kinetic attack, but it injured no one and the Iranians make no claim of irreparable physical damage.

But the US government apparently did view Olympic Games as a use of force. The strategic objective was not only to retard Iran's progress in developing nuclear weapons but to persuade Israel that using cyber weapons mooted the need for a kinetic attack on Tehran's nuclear institutions.*(16)* Both the G.W. Bush and Obama administrations strongly believed that Iran's nuclear-weapons programme had to be stopped. The United States has clearly felt a need to communicate that it would not tolerate Iranian intransigence. Former CIA Director Michael Hayden stated that:

> *This is the first attack of a major nature in which a cyberattack was used to effect physical destruction. And no matter what you think of the effects – and I think destroying a cascade of Iranian centrifuges is an unalloyed good – you can't help but describe it as an attack on critical infrastructure.(17)*

This implies that the Obama administration was willing in this case to affirm G.W. Bush's policy of pre-emption to deal with a threat deemed vital to national security interests, was willing to act in concert with a 'coalition of the willing' (even if the United States and Israel were the sole partners) to keep weapons of mass destruction out of the hands of rogue states,*(18)* and that this concern trumps commitments – including those expressed in the US 2011 Cyber

Strategy,*(19)* to embrace multilateralism and partnership for cyber strategy.

It seems evident that the intent of Olympic Games was to irreparably damage critical infrastructure. The tenor of the operation and strategic intent – and Hayden's words – strongly imply that White House and Department of Defense lawyers considered the operation a use of force. The issue must have been considered. One can presume the answer the lawyers provided was affirmative.

Legally, did the White House exceed its jurisdiction either under the Constitution, which reserves to Congress the right to declare war, or under the War Powers Resolution of 1973?*(20)* It is hard to qualify Olympic Games as an act of war. US statute defines that as armed conflict, whether or not war has been declared, between two more nations or between military forces of any origin.*(21)* It is significant that Iran has not suggested the use of Stuxnet constituted an act of war.

The War Powers Resolution offers a more nuanced issue. The resolution applies to the introduction of 'United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances'.*(22)* How does a nation use force except through military means? One can debate whether non-uniformed Stuxnet operations personnel qualify under the notion of distinction as combatants, but one can make a strong argument that Olympic Games fell under the ambit of the resolution. Presumably the response is that it constituted a covert action that did not trigger the operation of the law.

Given that the objective was to destroy an enemy's critical war-fighting capacity, though, one might wonder whether the logic in avoiding the jurisdiction of the resolution – or Congress's power to declare war – would apply to a modern Pearl Harbor. The air war in Libya may offer a clue to policy mindsets. Denying any obligation to ask Congress for authorisation to act, the Obama administration argued that 'U.S. operations do not involve sustained fighting or active exchanges of fire with hostile forces, nor do they involve ground troops'.*(23)* Similarly, Stuxnet did not involve armed fighting or exchanges of fire with hostile forces, although future engagements may focus debate on what constitutes armed forces. That cyber weapons often do not entail uniformed individuals firing rockets, dropping bombs, or firing guns does not, looking over the horizon, inherently render its users non-combatants.

What if Iran decided to respond kinetically? How does that alter the authority of the White House to continue a programme? Stuxnet was a fire-and-forget weapon. Although code can be designed to hit a specific target, in practice, once launched, there was no control over the consequences it inflicted – or upon whom. Indeed, Sanger reported that American officials were quite unhappy when Stuxnet got loose on the Internet.*(24)* The operational environment in war is random. The collateral effects of a cyber weapon add a new dimension to that challenge. One must think beyond the Iranian situation. What if Congress wanted a president to cease an operation that could not be terminated? Olympic Games side-stepped the problem, but hardly obscures the need for future strategic thinking.

Whether there was use of force raises other issues. Olympic Games involved a pattern of engagements. One must consider the larger implications of an individual event. Does a pattern convert employment of cyber weapons into a use of force? The answer isn't clear. The unpredictable nature of damage that cyber attack can inflict may require a new definition of war.

Intent may also matter in determining whether an engagement constituted a use of force. Open-source reporting indicates that any damage inflicted on the Natanz uranium-enrichment facility was temporary and reparable. But that was not the intent. What if someone dropped a bomb on London or New York that failed to detonate? Isn't that a use of force – or possibly, depending on the facts, an act of war? Deciphering intent may pose a challenge, but in law it may be objectively inferred. The case of unexploded ordinance seems easier to grasp, but how deep is the distinction between that and a cyber worm that fails? This issue needs debate and should enter future strategic calculations.

Finally, did Article 51 of the UN Charter justify Olympic Games? Like 'force', 'armed attack' remains undefined, even where force is clearly employed. Certainly the implications of new technologies for Article 51 or other international conventions remain unclear. This consideration matters enormously to Israel, which contends that a nuclear first strike would

destroy the nation, preventing or mooting a response. Washington worries about Israeli security, but also a potential and de-stabilising Middle East arms race should Iran acquire a nuclear weapon.

Strategic implications

The use of malware by state actors has altered the realities of cyber attack. History teaches that once weapons technology becomes feasible, states deploy it. Today the world may confront a dangerous technology race characterised by rapidly evolving and lethal weapons.

Clausewitz believed that in warfare, the advantage rested with the defence. Cyber reverses that equation. It also offers the potential to build the fog of war through the ability to effect disruption, deception, confusion and surprise. We are only beginning to envisage the potential for different forms of malware, or the strategies or tactics employed to use it.

A cyber-security tool may require millions of lines of code and a complex system to track and identify events. Malware requires a lot less. Computer code can be designed to evolve rapidly, mutating faster than defences can be mustered. Code can be highly targeted. It can leverage social and technological vectors. It can render a cyber defence obsolete within seconds. It can overwhelm a system that may have taken years to construct. Clausewitz believed that the advantages enjoyed by defence required that an offense employ greater resources. Cyber reverses that equation. Nations may now shift away from a refusal to use cyber weapons for first strike. That in and of itself complicates both offensive and defensive strategies.

Although some have argued that Olympic Games lowered the threshold for the use of cyber weapons, it may in fact actually raise it. States may recognise a higher responsibility to design weapons that offer strong assurance of striking only the intended targets. That was the intent of Stuxnet's planners and designers. But matters could have worked out much differently. Robert Burns was right: the best laid plans of mice and men often go awry.

Stuxnet shows that creating effective malware turns on imagination, technical expertise and ingenuity. But to deliver code as a warhead also requires highly specific domain experience and superior intelligence capabilities that often only states possess. Our view is that malware is not a wide-area weapon. As it evolves, it will be used narrowly to attack particular targets and to generate specific shaping effects.

Olympic Games raises the veil on key strategic implications. Stuxnet aimed to destroy a specific capability. But it importantly illustrates the political nature of war. Achieving a strategic political objective does not necessarily require destroying an enemy. Olympic Games was devised when G.W. Bush pushed for an alternative to the unpleasant choice between allowing Iran to develop a nuclear-weapons capability or halting the programme through kinetic attack. The cyber programme bought time in which to employ punishing sanctions and to signal to Iran that other nations would not tolerate an Iranian nuclear-arms programme. The lesson is that cyber weapons may offer non-kinetic ways to disrupt an operational capability of an adversary.

Future cyber weapons will similarly aim to constrain the ability of an adversary to manoeuvre, coordinate or synchronise, and to divert enemy commanders from focusing on the achievement of their own objectives. Stuxnet succeeded splendidly in creating confusion. Sanger reports that Iranians came to distrust their own instruments. The idea, he quotes one source, 'was to mess with Iran's best scientific minds' and 'make them feel they were stupid'.*(25)*

Conceptually, unsettling the consciousness of an adversarial commander, or a CEO or government official, causing a loss of belief in his ability to control events and depriving him of control, helps disrupt an adversary's ability to fulfil its objectives. Stuxnet's creators merit high marks for recognising the value of that goal. While the final result fell short, open-source reporting indicates that Stuxnet did retard Iranian progress.

As reported in open sources, Olympic Games exemplified an operation intended to reduce the resistance of a rival system and to inflict attrition upon its resources. Destruction of an asset is one of many potential objectives that cyber weapons can achieve. Future cyber weapons may disrupt communications systems or the ability of adversaries to cohesively operate air, naval or ground forces. They could slow the speed at which an adversary is able to mass forces or deploy assets, destroying precious momentum vital for an adversary's

offense.*(26)* Indeed, smart strategy is often less about destroying an enemy than paralysing command and control, and neutralising an adversary's operational ability.

One unfortunate development has been the leaks from Washington and Israel (where sources have long claimed credit for Stuxnet) about Olympic Games. These present a strategic challenge. An obstacle confronting any nation that wishes to retaliate against a cyber intrusion is the need to identify the intruder. The leaks solved that problem for Iran, and opened the United States and Israel to potential counterpunches that would entail far less stigma for Tehran than action against a putative attacker whose guilt could not be confirmed.

Finally, it is worth noting that the weapons employed by Olympic Games are largely indistinguishable from the technology that cyber criminals employ. That will make international treaties and conventions aimed at limiting cyber crime more difficult to secure. The utility and effectiveness of these weapons for national-security interests may trump policy considerations that favour better global policing of cyber crime.

There has been a widespread view that criminal entrepreneurs or state-sponsored proxies, acting at arm's length to insulate states from culpability for their policies, would emerge as the real challenges in a cyber era in which one individual can change the way the world does business. But now it seems that state-to-state engagement, whether or not it meets the conventional definitions of the use of force or an act of war, will define a new reality and require new strategic calculations. The discourse arising out of reports about Olympic Games underscores why the United States and other countries should engage in a transparent debate over whether or how cyber weapons should be employed. Every nation – including civilian as well as government institutions – must develop strategies to address these new realities.

Notes

This article first appeared in Survival: Global Politics and Strategy*, vol. 54, no. 4, August–September 2012, pp. 107-120.*

1 David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', Washington Post, 1 June 2012. Sanger lays out his report in Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power (New York: Crown, 2012), ch. 8. Although some wondered whether the White House had foolishly leaked the story, Sanger's book makes clear that he had access to sources with insider knowledge. He makes clear that former CIA Director Michael Hayden refused to discuss what he knew while holding that job and that, far from wanting to leak the secret, President Barack Obama wanted to preserve its secrecy.

2 The Jerusalem Post reported that Israel created both. 'Israel Admits to Waging Cyber War on Iran', Fars News Agency, 29 May 2012. See also Ellen Nakashima, Greg Miller and Julie Tate, 'U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say', Washington Post, 19 June 2012.

3 Nick Hopkins, 'Computer Worm that Hit Iran Oil Complex "is Most Complex Yet"', Guardian, 28 May 2012, http://www.guardian.co.uk/world/2012/may/28/computer-worm-iran-oil-w32flamer.

4 Sanger, Confront and Conceal, Kindle location 3108/7721.

5 Eligible Receiver was a 1997 US operation to test US Department of Defense planning and crisis/action capabilities when faced with attacks on DoD information structure. It revealed significant vulnerabilities to cyber attack and led to a new focus on cyber security. A breach of US military classified systems by the Agent/btz worm led to a Pentagon effort, Operation Buckshot Yankee, to disinfect worms. The operation led the armed forces to revamp information defences and create the US Cyber Command. See Kim Zetter, 'The Return of the Worm that Age the Pentagon', Wired, 9 December 2011, http://www.wired.com/dangerroom/tag/operation-buckshot-yankee/.

6 'Department of Defense Strategy for Operating in Cyberspace', July 2011, http://www.defense.gov/news/d20110714cyber.pdf. Integrated capabilities employed a holistic, whole-of-government approach to rapidly deliver and deploy innovative capabilities is also central to the strategy.

7 Computer Fraud and Abuse Act, 18 USC 1030.

8 See Sherman Antitrust Act (Sherman Act), 15 USCA 1-7, as amended by the Clayton Anti-Trust Act of 1914, 15 USC 12 et seq, notably Section 1(a); the Federal Trade Commission Act of 1914, 15 USCA 45 et seq, notably Section 5 that applies to unfair methods of competition. The Sherman Act prohibits business activities that reduce competition in the marketplace and requires the federal government to investigate and pursue trusts, companies and organisations it suspects may violate the act. It makes illegal contracts, combinations in the form of trusts or otherwise, or conspiracy, in restraint of trade or commerce. The FTC Act authorises the commission to enforce the anti-trust laws.
9 18 USC 2510, et seq and18 USC 2701-12. This legislation deals with protecting the privacy of stored electronic communications. The PATRIOT Act, 18 USCA 1 (Pub. L. 107-56, 107thCongress) et seq, arguably weakened some provisions of the ECPA.
10 Steve Ragan, 'U.S. Confirms it Will Use Military Force in Response to Cyber Attacks', Tech Herald, 22 November 2011: http://www.thetechherald.com/articles/U-Sconfirms-it-will-use-military-force-inresponse-to-cyber-attacks.
11 Prepared answers of Lieutenant-General Keith Alexander, nominee for commander, US Cyber Command, Senate Armed Services Committee, 15 April 2010, p. 24, available at http://www.fas.org/irp/congress/2010_hr/041510alexander-qfr.pdf.
12 Kevin G. Coleman, 'Cyber Rules of Engagement – Hot Pursuit', InfoTech Spotlight, 18 August 2009: http://it.tmcnet.com/topics/it/articles/62417-cyber-rules-engagement-hot-pursuit.htm.
13 See United States v Santana, 427 US 38 (1976).
14 See for example Nicholas M. Poulantzas, The Right of Hot Pursuit in International Law, 2nd ed. (The Hague: Kluwer Law International, 2002), p. 3.
15 Abraham M. Denmark and James Mulvenon, Contested Commons: The Future of American Power in a Multipolar World (Washington DC: Center for a New American Security, 2010), p. 7.
16 See James P. Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', Survival, vol. 53, no. 1, February–March 2011, pp. 23–40. The article summarises the debate on whether a kinetic strike against Iran made the most sense.
17 Sanger, Confront and Conceal, Kindle location 3215/7721.
18 See Jon Rosenwasser, 'The Bush Administration's Doctrine of Preemption (and Prevention): When, How, Where?', Council on Foreign Relations, 1 February 2004, http://www.cfr.org/world/bush-administrationsdoctrine-preemption-prevention-/p6799.
19 Department of Defense Strategy for Operating in Cyberspace, July 2011, http://www.defense.gov/news/d20110714cyber.pdf. The 4th StrategicInitiative it sets forth emphasises the need to 'build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity' (p. 9). The language is especially relevant as the United States views Iranian acquisition of nuclear weapons as a global threat, not one merely to the United States or Israel.
20 50 USC 1541–48.
21 See 18 USC 2331.
22 50 USC 1542.
23 Charlie Savage and Mark Landler, 'White House Defends Continuing U.S. Role in Libya Operation', New York Times, 15 June 2011, http://www.nytimes.com/2011/06/16/us/politics/16powers.html.
24 Sanger, Confront and Conceal, Kindle locations 3279–87/7721.
25 Ibid., Kindle location 3206/7721.
26 See Shimon Naveh, In Pursuit of Military Excellence: The Evolution of Operational Theory (New York: Frank Cass Publishers, 1997). A retired Israeli Defense Forces Brigadier, General Naveh is a strong proponent of operational strategies that achieve these objectives in a systematic, cohesive manner. This section of the paper adapts some of his ideas.

James Farwell *is an expert in strategic communication and has advised the Department of Defense on strategic and political issues in the Middle East. He is author of The Pakistan Cauldron: Conspiracy, Assassination & Instability (Washington: Potomac Books, 2011) and the forthcoming Persuasion & Power (Washington: Georgetown University Press, 2012.*

Rafal Rohozinski *is a principal and CEO of the SecDev Group. He is a cofounder and principal investigator of the Information Warfare Monitor and OpenNet initiative, and author of numerous papers and studies addressing risk and the nexus*

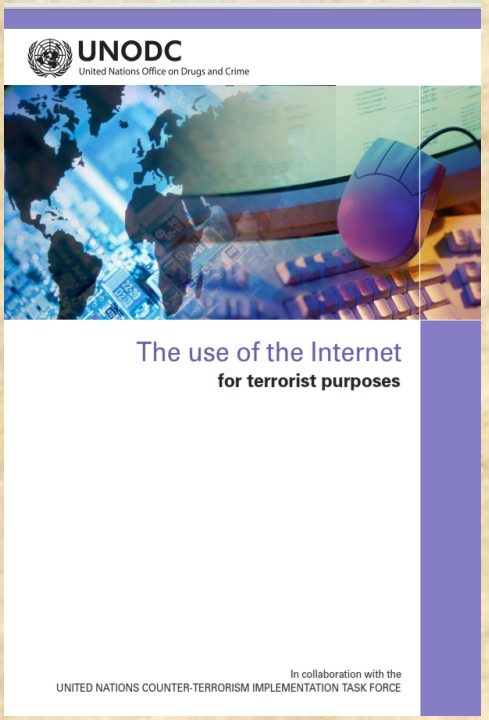
between conflict, development, and the emerging global cyberspace domain. He was previously the director of the Advanced Network Research Group, Cambridge Security Programme, University of Cambridge. The views expressed are those of the authors and do not represent those of the U.S. or Canadian Governments, their departments, agencies, or armed forces.

The UN report on the use of the internet for terrorist purposes

Source: http://www.infosecurity-magazine.com/view/29051/the-un-report-on-the-use-of-the-internet-for-terrorist-purposes

The United Nations Office on Drugs and Crime, with "the generous support of the Government of the United Kingdom", has published a report of almost 150 pages titled 'The use of the Internet for terrorist purposes'.

In some senses the title is misleading – something that F-Secure's Mikko Hyponnen hints at. Most people associate cyberterrorism with cyberattacks; but that is an area specifically excluded. One reason may be that many members of the UN are already engaged in such activity against other members (such as the US-sponsored Stuxnet attack agaiinst Iran), making it a difficult subject to tackle objectively. "While a considerable amount of attention has focused in recent years on the threat of cyberattacks by terrorists, that topic is beyond the scope of the present publication and, as such, will not be a subject of analysis," notes the UNODC report. Hyponnen comments, "a little bit disappointingly the document does not go deeper into the potential of actual online attacks launched by such groups."



The real purpose of the report is to discuss how the internet 'supports and promotes' terrorist activities rather than how it is used to deliver terrorist attacks. This is made clear in the foreword by Yury Fedotov, the executive director of the UN office on drugs and crime. The purpose of the report is, "first, to promote a better understanding of the ways in which communications technologies may be misused in furtherance of acts of terrorism and, second, to increase collaboration among Member States, so that effective criminal justice responses to this transnational challenge can be developed."

It is, effectively, a justification for, followed by a description of, the type of legislation increasingly demanded by national governments. This too is made clear in that part of the foreword provided by Richard Barrett, co-chair of the working group, saying he is confident that the report "will help to identify the legislative areas in which the United Nations can assist... Member States."

The report itself thus neatly falls into two parts: a discussion on how the internet is used by terrorists (excluding cyberattacks), followed by a discussion on legislative (and self-regulatory agreements) that can be used to thwart such activities.

"In addition to using the Internet to plan and finance terrorist acts," summarizes the report, "terrorists also use it to recruit and train new members; communicate, research or reconnoitre potential targets; disseminate propaganda; and incite others to carry out acts of terrorism." The proposed response is to ensure the clear illegality of such activity, to give necessary communications interception capabilities a legal basis (while respecting citizens' privacy and human rights), and to promote active international and intranational co-operation.

International co-operation is required between different nations and their law enforcement agencies. "Timely and effective international cooperation between law enforcement and intelligence agencies [is] an increasingly critical factor in the successful investigation and prosecution of many terrorism cases."
Intranational co-operation is between law-enforcement and national internet stakeholders, including service providers. For example, "Recommended measures to be taken by law enforcement authorities pursuant to the guidelines" includes the comment that ISPs should provide a list "of which types of data could be made available for each service to law enforcement, upon receipt of a valid disclosure request."
"We hope," say the UK's Simon Shercliff (counter terrorism ops) and Sue Hemming OBE (Crown Prosecution Service), that this report "will rapidly become a useful tool for legislators, law enforcement officials and criminal justice practitioners to develop and implement legal frameworks that will effectively disrupt terrorists' activities online."

► **Read full report at:**
http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Michigan launches Cyber Range – a cutting-edge cybersecurity training program

Source: http://www.homelandsecuritynewswire.com/dr20121112-michigan-launches-cyber-range-a-cuttingedge-cybersecurity-training-program

Governor Rick Snyder of Michigan the other day announced the opening of the Michigan Cyber Range, a state-of-the-art facility that prepares cybersecurity professionals in the detection and prevention of cyber attacks.
It is a partnership between the state of Michigan, Merit Network, federal and local governments, colleges and universities, and the private sector. The initiative pairs cybersecurity resources with hands-on training opportunities to enhance Michigan's protection of computer systems and sensitive data.
"Every day, breaches to computer systems threaten the security of data - data that may include personal information about Michigan's citizens," Snyder said. "This partnership to establish the Michigan Cyber Range benefits all levels of government as well as educational systems, private businesses and industry."

Hosted by Merit Network, the Michigan Cyber Range enables individuals and organizations to develop detection and reaction skills through simulations and exercises. The program offers students and Internet technology professionals a full curriculum of meetings and workshops as well as critical cybersecurity training and awareness tools.
The governor said the new cyber range would serve as a central resource hub and a partner in innovation and collaboration. Aareas that will benefit from the creation of the Michigan Cyber Range include:

- Infrastructure defense
- Homeland security
- Criminal justice and law enforcement
- Academic and educational programs and curricula related to information and communications technology
- Entrepreneurial, small and medium businesses in the private sector

"The cyber threat is certainly one of the - if not the - largest threat that we face today," said Don Welch, Merit Network president and CEO. "In a cyber attack, we must rely on trained professionals, and the new cyber range provides a unique training experience that cannot be replicated in other settings. It's important to arm cyber professionals with training and the most current resources available, and that's exactly what we are doing with this effort."
Students using the cyber range can perform laboratory exercises and out-of-class work that uses the cyber

range's virtual environment and text, video chat and Web conferencing capabilities.

"The Michigan Cyber Range will provide a capability not found anywhere else in the world," said John Nixon, director of the state's Department of Technology, Management and Budget. "In Michigan, we have a governor who understands the importance of safeguarding our resources. His commitment will ensure that a broad range of cybersecurity professionals have access to current methods and resources."

Initially, the cyber range's physical assets will be housed at Eastern Michigan University.

Additional sites are planned for Ferris State University and the 110th Airlift Wing in Battle Creek. With additional funding, expansion plans could involve as many as ten sites.

The Michigan Cyber Range is part of Michigan's cyber initiative launched last fall to improve cybersecurity efforts to protect families, communities, businesses and government.

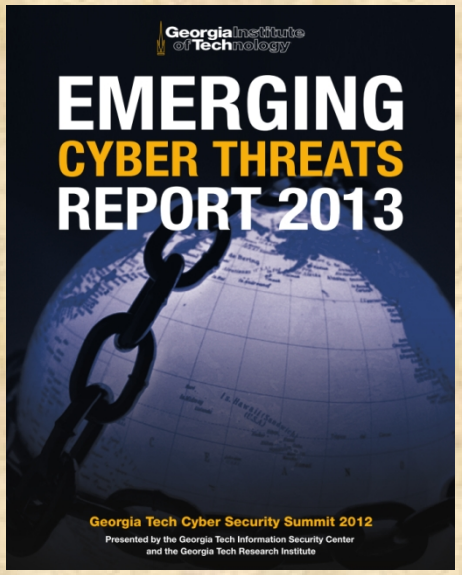
Michigan Cyber Range partners include Merit Network, U.S. Department of Homeland Security, U.S. Department of Energy, National Institute of Standards and Technology, DTE Energy, Consumers Energy, Plante and Moran PLLC, Juniper Networks, Eastern Michigan University, Michigan State Police, Michigan Department of Military and Veterans Affairs, Michigan Economic Development Corp., and the Michigan Department of Technology, Management and Budget.

Merit Network, a nonprofit corporation governed by Michigan's public universities, owns and operates America's longest running regional research and education network and supports the high-performance networking needs of Michigan's universities, colleges, K-12 schools, libraries, state government, health care and other nonprofit organizations.

Georgia Tech releases cyber threats forecast for 2013

Source: http://www.homelandsecuritynewswire.com/dr20121115-georgia-tech-releases-cyber-threats-forecast-for-2013

The year ahead will feature new and increasingly sophisticated means to capture and exploit user data, escalating battles over the control of online information and continuous threats to the U.S. supply chain from global sources. Those were the findings made by the Georgia Tech Information Security Center (GTISC) and the Georgia Tech Research Institute (GTRI) in this week's release of the Georgia Tech Emerging Cyber Threats Report for 2013. The report was released at the annual Georgia Tech Cyber Security Summit, a gathering of industry and academic leaders in the field of cyber security.



A Georgia Tech release reports that aAccording to GTISC, GTRI, and the experts cited in the report, specific threats to follow over the coming year include, among others:

- *Cloud-based Botnets* — The ability to create vast, virtual computing resources will further convince cyber criminals to look for ways to co-opt cloud-based infrastructure for their own ends. One possible example is for attackers to use stolen credit card information to purchase cloud computing resources and create dangerous clusters of temporary virtual attack systems.
- *Search History Poisoning* — Cyber criminals will continue to manipulate search engine algorithms and other automated mechanisms that control what information is presented to Internet users. Moving beyond typical search-engine poisoning, researchers believe that manipulating users' search histories may be a next step in ways that attackers use legitimate resources for illegitimate gains.
- *Mobile Browser and Mobile Wallet Vulnerabilities* — While only a very small number of U.S. mobile devices show signs of infection,

the explosive proliferation of smartphones will continue to tempt attackers in exploiting user and technology-based vulnerabilities, particularly with the browser function and digital wallet apps.

- *Malware Counteroffensive* — The developers of malicious software will employ various methods to hinder malware detection, such as hardening their software with techniques similar to those employed in Digital Rights Management (DRM), and exploiting the wealth of new interfaces and novel features on mobile devices.

"Every year, security researchers and experts see new evolutions in cyber threats to people, businesses and governments," said Wenke Lee, director of GTISC. "In 2013, we expect the continued movement of business and consumer data onto mobile devices and into the cloud will lure cyber criminals into attacking these relatively secure, but extremely tempting, technology platforms.

Along with growing security vulnerabilities within our national supply chain and healthcare industry, the security community must remain proactive, and users must maintain vigilance, over the year ahead."

"Our adversaries, whether motivated by monetary gain, political/social ideology or otherwise, know no boundaries, making cyber security a global issue," said Bo Rotoloni, director of GTRI's Cyber Technology and Information Security Laboratory (CTISL). "Our best defense on the growing cyber warfront is found in cooperative education and awareness, best-of-breed tools and robust policy developed collaboratively by industry, academia and government."

► **Read the report at:** http://www.gtsecuritysummit.com/pdf/2013ThreatsReport.pdf

Locations of Hamas Leaders Identified during Qatari Emir's Recent Visit to Gaza

Source: http://english.farsnews.com/newstext.php?nn=9107119940

TEHRAN (FNA) – The residence and offices of a number of Hamas leaders were identified during the recent visit to the Gaza Strip by Qatar's King Sheikh Hamad bin Khalifa Al Thani and later targeted by Israeli missile and bomb attacks, informed sources disclosed.

The emir of Qatar gifted a number of watches and ballpoint pens to Hamas leaders, which transmitted low-frequency signals to Israeli satellites, the sources, who asked to remain unnamed due to the sensitivity of the information, told FNA, adding that the Israeli military officials would then use the received signals to spot and assassinate senior Hamas officials.

Sheikh Hamad arrived in Gaza on October 23 to become the first head of state to visit the besieged enclave since the Palestinian resistance movement, Hamas, took power in the territory five years ago.

Qatar's emir has repeatedly met with Israeli leaders, and is working hard to boost the diplomatic clout of his small Persian Gulf country.

The Israeli military frequently carries out airstrikes and other attacks on Gaza Strip. The new wave of Israeli aggression on the Gaza Strip has claimed more than 41 lives since November 14. Ahmed al-Ja'abari, the popular and influential head of the Hamas military wing, the Ezzedeen al-Qassam Brigades, was assassinated in an Israeli attack on his car on Wednesday.

On Friday, Ahmed Abu Jalal, a field commander of the Ezzedeen al-Qassam Brigades, was also killed in an Israeli airstrike on the central Gaza district of Maghazi.

Israel cyber security incubator program established by Ben-Gurion University of the Negev

Source: http://www.homelandsecuritynewswire.com/dr20121212-israel-cyber-security-incubator-program-established-by-bengurion-university-of-the-negev

Ben-Gurion University of the Negev (BGU) and its technology transfer company, BGN Technologies, will create Israel's first cyber security incubator in Beer-Sheva under the Israeli Office of the Chief Scientist Incubator Program. The incubator program will be established in partnership with Israeli venture capital firm Jerusalem Venture Partners (JVP).

"The exciting initiative is taking place in the wake of rising cyber threats, as well as increasing attacks on critical infrastructure in Israel and around the world," says Doron Krakow, executive vice president, American Associates, Ben-Gurion University of the Negev. "BGU is one of the leaders in academic applied research in cyber security, which is a critical component of our Homeland Security Institute."

The incubator will be located in the new Advanced Technologies Park, adjacent to both the University and the new technology campus of the Israel Defense Forces Telecommunications Division. The incubator is expected to begin operations as early as the beginning of 2013.

JVP will select a number of start-ups each year within the cyber security and enterprise software areas to join the incubator. Once established, the incubator will also include another incubator for community-based social initiatives and a cultural arm.

Israel has been named one of the top three world leaders in the field of cyber security. Approximately twenty-five Israeli information security firms have been acquired by multinational organizations, and Israeli companies are counted among the world's leading IT security providers.

"High-tech is the engine of the Israeli economy, and it's important that we bring it to areas and population groups throughout the country," said JVP founder and chairman Erel Margalit.

"Israel's leadership in the area of cyber security is a strategic asset for the country, and we can leverage it not only for security purposes, but also economically and socially. Establishing the Beer-Sheva incubator alongside a social incubator and other cultural hotspots can create cultural and social change along with a thousand new jobs."

JVP's Yoav Tzruya, who will be heading the cyber security incubator, says that "Our vision is to turn Beer-Sheva into a center of innovation and creativity in the field of high-tech, and a leader in the field of cyber security."

Cybersecurity company using hackers own devices against them

Source: http://www.homelandsecuritynewswire.com/dr20121213-cybersecurity-company-using-hackers-own-devices-against-them

Shawn Henry, the head of the FBI cyber crimes division, this year left agency after twenty-four years to become the president CrowdStrike, an Internet security start-up in Irvine, California.

In his government work, Henry often new what foreign governments were involved in hacking the computer network of American companies, but could not share this information with the irate leaders of the hacked companies because the information was classified.

The *Los Angeles Times* reports that now, CrowdStrike, which is marketing itself as a private cyber intelligence agency, works to identify foreign attackers who are attempting to steal corporate secrets. It does so by using the attackers' own techniques and vulnerabilities against them. The company also collects data on hackers and tricks intruders into stealing false information.

This kind of reverse hacking has opened up an ethical debate about

how far a company should go to prevent an attack.

"The traditional way of trying to defend your network is just not going to cut it. You have to do something different," Irving Lachow, who directs the Program on Technology and National Security at the Center for New American Security, told the*L.A. Times.*

"One way is to engage the adversary. CrowdStrike represents a new breed of company that is focused on doing exactly that," Lachow added.

When somebody is shooting at you, "you don't ask, 'Is that a 9-millimeter or a .45,'" CrowdStrike CEOGeorge Kurtz told the *Times*. "You ask: 'Who is shooting at me and why are they shooting at me?'"

Kurtz, a former chief technology officer at McAfee Inc. started CrowdStrike earlier this year with another former McAfee employee Dmitri Alperovitch.

The *Times* notes that Alperovitch gained notoriety last year when he wrote a paper on what he described as Operation Shady Rat, a series of state-sponsored cyber penetrations of more that seventy U.S. government institutions, agencies, and companies. Alperovitch did not name China as being behind the attacks, but to experts who the paper there was no need to spell this out.

Attackers often breach networks using a method known as spear phishing, which involves getting an employee to download a malware file by disguising it. An e-mail that looks as if it was sent by someone the employee knows is the way most hackers hide the file. This method can render anti-virus programs and firewalls useless.

CrowdStrike uses decoys as a trap to lure hackers into an environment where investigators then watch and trace the attack. In some cases the company will feed the hacker false information.

CrowdStrike also has people who can read and write in Chinese, as well as former employees of the U.S. government who worked in cybersecurity. These men and women are able to identify Chinese hackers using clues in their malware and profile them with real names and photos.

The company does have its critics, who fear that the company could take the program too far.

"You don't want the Internet to resemble Somalia," one cyber expert who did not want to be identified because it could jeopardize his friendships with CrowdStrike's founders told the *Times*.

"We will not break the law, but there's a lot organizations can do behind their own firewall on their own networks to make life difficult for the adversary," Henry told the *Times*.

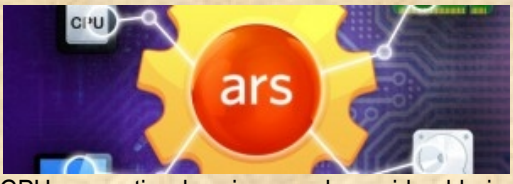
Critics also worry about the extent to which CrowdStrike runs it operations against hackers that are controlled by the Russian and Chinese governments, saying that it could lead to an international incident.

Alperovitch had a response for those critics.

"Why isn't it an international incident when China steals our intellectual property? Alperovitch told the *Times*. "If the government would say, 'We're actually going to stand up to China,' that would be great; we'd go back to doing defense only. But they are not saying that."

Expert show how to crack every common password in under six hours

Source: http://www.homelandsecuritynewswire.com/dr20121213-expert-show-how-to-crack-every-common-password-in-under-six-hours



GPU computing has improved considerably in recent years, and Jeremi Gosney, founder and CEO of Stricture Consulting Group, used a 25-GPU cluster that can run through 350 billion guesses per second to show how easy it would be to crack practically any password out there (easy, that is, if you can use a 25-GPU cluster).

Arstechnica reports that Gosney demonstrated his feat last week during the Passwords^12 Conference in Oslo, Norway.

The 350 billion guesses happen when cracking the NTLM cryptographic algorithm found in every Windows OS since Server 2003. The cluster can try

an astounding 95^8 combinations in just 5.5 hours, enough to brute-force every possible

eight-character password containing upper- and lower-case letters, digits, and symbols.

The GPU cluster uses the Virtual OpenCL cluster platform to let each card function as if on a single desktop, plus ocl-Hashcat Plus which runs on top to allow the running of forty-four other algorithms. Gosney noted that Dictionary and other attacks can also be run, so the machine does not have to rely solely on brute force to crack a password. "Aattack hashes approximately four times faster" than before, he said.

He noted that these speeds only apply to offline attacks against a database of lifted passwords stored with a one-way cryptographic hash, but cannot be used in online attacks as Websites restrict the number of guesses.

Arstechinca notes that this cluster has limitations against different algorithms. "Fast" algorithms, like SHA1, SHA2, SHA3, and MD5, can be cracked fairly quickly, while ones like Bcrypt, PBKDF2, and SHA512crypt are much harder. A mere 71,000 guesses per second can be made against Bcrypt while 364,000 guesses against SHA512crypt are possible, which are both vastly better than the "fast" algorithms.

Arstechnica offers its readers this advice about password security:

> *For the time being, readers should assume that the vast majority of their passwords are hashed with fast algorithms. That means passwords should never be less than nine characters, and using 13 or even 20 characters offers even better security. But long passwords aren't enough. Given the prevalence of cracking lists measured in the hundreds of millions, it's also crucial that passwords not be names, words, or common phrases. One easy way to make sure a passcode isn't contained in such lists is to choose a text string that's randomly generated using Password Safe (link below) or another password management program.*

► **Visit Password Safe at: http://passwordsafe.sourceforge.net/**

Is the US health care system a target for cyberterrorism?

Source: http://www.kurzweilai.net/is-the-us-hea

Cyber threats are on the rise, and U.S. health care organizations must be better prepared to deal with them, according to an open-access article in *Telemedicine and e-Health*.

The health care system in the U.S. is a $2.5 trillion industry and depends heavily on communication and the transfer of information via the Internet. This puts it at ever-increasing risk of a cyberterrorism attack, which could jeopardize lives and threaten patient care and privacy, the authors point out.

What Is the risk for Healthcare Targets?

The risk has become more acute in larger healthcare organizations such as hospitals, which have moved away from stand-alone workstations to more tightly integrated platforms attached to networks, according to the authors. It is now common for these networks to link a variety of IT workstations such as admissions, clinical laboratory, pharmacy, radiology, and the billing department.

Networks also connect the IT systems of an organization's inpatient and outpatient settings as well as a variety of service organizations ranging from acute care to long-term care and home care.

These systems also have links to external networks, which connect and share information with patients, employees, insurers, and business partners. Areas of particular concern to healthcare-related facilities include the potential for cyberterrorism-related events to erase or alter computerized medical, pharmacy, or health insurance records.

Scenario

If terrorists were to attack America's healthcare IT systems, it probably would not be through the use of one major assault, but rather via a series of small incursions that are much more difficult to detect, the authors suggest. An example of this type of scenario was outlined recently in a cyberterrorism seminar at the University of California, Davis:

1. Hackers use "phishing" e-mails to introduce four separate packages of malware into the hospital networks. Once planted, these packages trigger in sequence a few days or weeks apart. The first infects patient record databases and alters doctors' orders, medication doses, and other information, spreading confusion and possibly causing illness and deaths.
2. A few days later, the next program triggers, interfering with portable devices that nurses use to record patient information.
3. The third wave attacks the software in intensive care unit monitors, altering the data display and switching off alarms.
4. The fourth and final wave infects the software controlling drug infusion pumps and similar devices.
5. After a few weeks of these rapidly changing, and different, attacks, the staff in the hospital has no trust in any electronic data, and the IT support staff is totally demoralized.