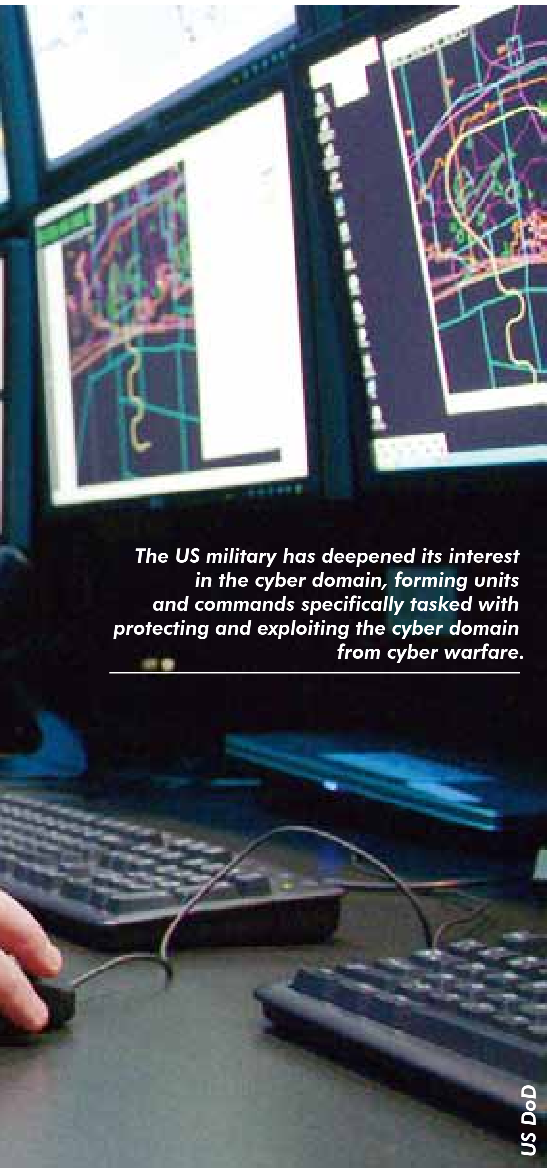
WEB OF INTRIGUE

With perhaps the exception of infectious disease, no other security challenge is perhaps as pervasive and universal as those proliferating from cyberspace. Every nation in the Asia-Pacific region, not least the world, is connected to the World Wide Web; yes even the Democratic People's Republic of Korea (DPRK).

by **Dr. Tom Smith**

The threats arising from the norm of hyper-interconnection are couched in a myriad of often confusing and overlapping terms and frames of reference. These range from those employed by the private sector, often referred to as cyber security to combat cyber crime, to cyberwarfare for the military to protect national interests, and then cyber terrorism (referred to hereafter as cyber insurgency) that demands everyone's attention but is perhaps not everyone's responsibility.

Given that these three distinctions—crime, warfare and insurgency—are crudely drawn (in part as a result of the structures of government and commerce), to complicate things further, they differ drastically from nation to nation for many different reasons. What is understood as a cyber crime in one domain can be considered cyber insurgency in the next. Politics and economics are obvious drivers of these distinctions but culture and technological literacy is also a key force that can partly level otherwise unbalanced ideological or financial playing fields.



The US military has deepened its interest in the cyber domain, forming units and commands specifically tasked with protecting and exploiting the cyber domain from cyber warfare.

US DoD

This is a topic as complex as it is compelling. Indeed because this topic is confusing, this is one of the reasons why such threats exist in the cyber domain. The language of this problem is in itself something we often have to learn from scratch and continually renew. This is not an arena where classical Clausewitzian military thinking readily lends itself to debates regarding the malicious use of computer software and such like, though we would do well to apply all the models we can to the problems before us. So while trying to divide the cyber problem up by way of national and polity boundaries, as is the regular response to most security concerns, often the response is a clumsy attempt to make a national solution out of a very international problem. Nations understandably are concerned about their cyber domain, but because their cyber domain is unable to be fenced off and patrolled, this presents a question of what are they trying to protect? Each nation is asking the same question of itself. Each shares the other's concerns and vulnerabilities, and the response has largely been to retreat and guard our own 'digital turf' in the best way we can.

Cyber-Crime

Seemingly some countries have more to lose than others, the valuable financial assets of developed nations heighten concern for these states. So when western companies cry foul over the cyber criminals stealing Intellectual Property (IP) from manufacturers, designers and other creatives in the sacred knowledge economy, Western governments act with the cyber crime units of national police organisations and alike. Though to what extent the US Department for Homeland Security can help Google in this regard is a question worth asking.

In 2015 a report published by PricewaterhouseCoopers, a British professional services company, for the UK government found the average cost of the worst cyber breaches at large UK organisations to be between $2 million and $3.1 million; eye watering amounts for single breaches. But the concern is shared in all nations; when internet access is the 21st century golden ticket to economic prosperity, developing nations need the same protection. This is therefore not an East versus West, North versus South or rich versus poor problem yet it is often implied that way. The poor may steal from the rich, but there are some awfully rich cyber criminals stealing from the poorest in the world. Then there are social crusaders such as the Algerian hacker Hamza Bendelladji who was arrested in Bangkok in 2013 and is, at the time of writing (April), currently being sentenced in a US court for the use of a malware (malicious software) programme called Zeus for stealing from US banks and giving the money to Palestinian charities.

From the inception of the networked computer and later the growth of the World Wide Web in the 1990s, crime like other human behaviours has both exploited and fuelled the need to interconnect. In the same way that crime Away From the Keyboard (AFK) or In Real Life (IRL) benefits from improved communication there is little surprise that the digital realm has become a domain and producer of new criminal enterprise. Data, the series of binary zeros and ones hidden inside a programming language, is the new treasure. This data is valuable outside of its hard drive, and beyond its user and intended purpose. Therefore, the desire for this new and increasingly valuable commodity is not just the new gold rush but perhaps the only gold rush in 21st century life, Bitcoin (an online virtual currency) included. Data is digital and however sophistically encrypted, is now nearly always accessible remotely: It is the outpost that can allow the criminal to tunnel straight to the main camp.

Given that the natural hub of analogue organised crime did not initially possess the skills to make the shift from IRL crime to cyber crime, the lone hacker had much of the digital landscape to themselves for a

YouTube

The Anonymous organisation has attacked many organisations, governments and corporations they believe to violate human rights or to practice censorship, and whose actions have received significant coverage.

The pan-European law enforcement organisation Europol is playing a significant role in combating the activities of cyber crime, fostering cooperation to this end across international borders.

Europol

short period. Today, organised crime very much does. With cyber crime the IRL distinction has blurred if not disappeared entirely. In the Asia-Pacific, the historic and well entrenched organised crime networks of the *Solntsevskaya Bratva* (Russian Mafia), various groups of the Chinese Mafia (Triads) such as the *Sun Yee On* and Japan's *Yamaguchi Gumi* (*Yakuza*) have shown the same criminal enterprise as they have in interests as varied as drug trafficking and sports betting. In August 2015 Jakarta Police crime directorate head Senior Commander Krishna Murti was explicit in his blame for transnational cyber crime undertaken in his domain. "The victims are mostly from the People's Republic of China and Taiwan. The network itself (is) protected by big (criminal) organizations in Japan such as the *Yakuza,*" he said.

Criminal enterprise changes over time as our behaviours change online, from credit card theft, to more sophisticated bribery and extortion often based on hacking email, social media and other accounts. The range of threat and target is wide, from individuals to companies, from financial data to sensitive personal data. Some tactics require only an independent programme others human interaction, some work with both. The DDB4C (Distributed Denial of Service for Bitcoins) group responsible for a string of attacks around the globe has required an 18-month campaign headed by Europol (the law enforcement agency of the European Union) to make arrests in 2016 following perhaps the most sophisticated extortion campaign yet seen.

The response globally and specifically in the Asia-Pacific has largely been the focus of the cyber security sector for individuals and companies to manage, usually by outsourcing to experts. The growth of the cyber security industry to protect online identities, encrypt the embarrassing family photos or the latest company design is inherently commercial. As the value of commoditized data rises seemingly inexorably there is a cost, a financial one, to our digital life and our digital trade. This creates a burden particularly painful to those without basic literacy in cyber security and for start-up enterprises in developing nations that require support. Even small enterprises in developing nations will suffer from weaker technical infrastructures and the lack of a culture of strong cyber security. Western companies were obvious first targets for the first generation of cyber criminals, but as their defences improve in response, vulnerabilities in growing Asia-Pacific markets is seen as a potentially softer target and no less profitable anymore. Indeed the lack of a Europol-style multinational law enforcement organisation in the Asia-Pacific equipped with cyber expertise is telling.

Cyber War

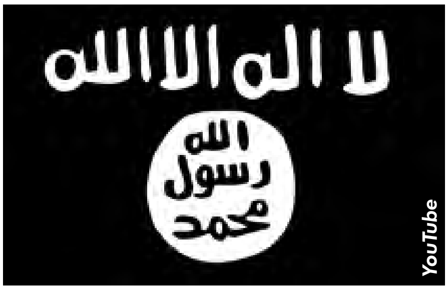
Where nations clash, the cyber domain like all others, is another arena for conflict for the 21st century. The first thing to note is that 'war' is something that is usually done in the open. What is being termed 'cyber war' has been fought largely behind closed doors and is really not war in any term we could conflate with notions of traditional warfare. Can countries be our enemies in cyberspace but our allies in all other spaces?

What do nations understand as an act of cyber war? This also remains unclear. The hacking of commercial data that leads to commercial losses on a large scale could certainly damage economic national interest and potentially be grounds for a national military response. Similarly a smaller scale sensitive theft from defence contractors could strike at the heart of a nation's security. But is this not old fashioned espionage made digital? Cyber war remains a phrase banded about but with little application.

Cyber war between states as well as between the many non-state actors active in the cyber domain raises more questions than answers. Are those fighting cyber war concerned about cyber crime? Is the commercial threat something which militaries in the Asia-Pacific are cognizant of? If so, at what point do these attacks become war? And this is all before we get to the other half of the issue, namely how do we fight back? With cyber? Can this avoid civilian casualties? With conventional force? Is that proportionate? These, and many other questions, have lead to increasing amounts of scepticism in the cyber community about what is said and meant to be cyber warfare.

Evgeny Morozov, who studies the political and social implications of technology, and author of *To Save Everything Click Here* and *The Net Delusion*, has described how the debate on cyber war is "packed with cyber-jingoism from former and current national security officials." But when people like the Director of the Central Intelligence Agency Leon Panetta claim that "the next Pearl Harbour is likely to be a cyber attack going after our grid" people take notice. The noted commercial interests in cyber crime are also found in cyber warfare with a number of government contractors providing expertise to militaries which have lead to accusations of threat inflation. To Mr. Morozov "cyberwar is the new 'dog ate my homework' (excuse). It's far easier to blame everything on mysterious Chinese hackers than to embark on uncomfortable institutional soul-searching."

For its part the White House under President Barack Obama has tried to bring clarity. "America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas," Mr. Obama stated in 2014.



ISIS has been adept at using the Internet both for the performance of cyberattacks, but also for propaganda purposes and as a powerful recruitment tool.

The PRC's response has been equally measured. Xi Jinping, the PRC's President during a September 2015 visit to the White House agreed stating that "commercial cyber theft against government networks are crimes that must be punished in relevance to international treaties." Mr. Xi added that "(t)he international community should work to ensure a peaceful and open cyber security space." Agreement between the US and the PRC on implementation and making any of the common ground into reality has yet to surface. Is it in a nation's interest to remove the tool of cyber warfare from their arsenal? For now it seems not, and the risk of cyber turning kinetic, physical or IRL (however we wish to disguise it) has been made very clear. "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country," noted the US International Strategy for Cyberspace in 2011. "We reserve the right to use all necessary means, diplomatic, informational, military, and economic, as appropriate and consistent with applicable international law, in order to defend our nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible," the strategy continued.

Cyber Insurgency

Somewhere between the previous two subsets of 'the cyber problem' is another popular used and abused term, 'cyber-terrorism'. As a general rule *AMR*, prefers to avoid the term 'terrorist' or 'terrorism' which we believe has the potential to be value-laden. However, for the sake of clarity, we will take the non-state actor as the cyber insurgent, but under the proviso that states (and criminals for that matter) are perfectly capable of using insurgency as a tactic. Groups or individuals using many of the same cyber vulnerabilities exploited in crime and potentially in warfare are capable of committing the same attacks but for different reasons. Financial gain, economic superiority or technological advantage can be replaced by politics, ideology, religion and the myriad of motivations for insurgent actions.

When the Stuxnet computer worm (widely believed to have been developed by US and Israeli computer experts) hit the Iranian nuclear facility at Natanz, central Iran in 2010, the obvious repercussions caused seismic waves throughout the international security community. Stuxnet was designed to infect and alter computer-controlled electro-mechanical processes. There is obvious motivation for such acts to be carried out by other states wishing to hinder Iranian nuclear proliferation, but the warning that such acts are possible raised the stakes of such an act for non-state actors with technical expertise and motivation.

The other sphere when it comes to cyber insurgency is when 'traditional' IRL terrorist groups use the cyber domain to their advantage. Much has been made of the blatant use of web technologies by the Islamic State of Iraq and Syria (ISIS) insurgent group, be it through social media and the dark web for propaganda networking but also in the adoption of encrypted messaging. For now these have been framed in a way as to support the IRL activates, to generate revenue, support and foreign fighters for physical conflict in Syria and elsewhere.

Across the Asia-Pacific, despite regional cooperation by the likes of ASEAN (the Association of South East Asian Nations), there are considerable rivalries that for now prevent the regional collaboration on enforcement that you see in Europe or even the dialogue pursued by competing nations such as the US and PRC as noted above. The old, and somewhat true, adage that 'Free Trade Stops Wars' could be revised here as a principle to deter cyber war. This could be done if cyber cooperation is understood as the foundation on which trade and ultimately peace is based upon. AMR