Preventing illicit trade in dual-use items & technologies

The author of this article, Ian Stewart, runs Project Alpha—an initiative based at King's College London that works to understand and counter illicit trade in proliferation-sensitive goods. This includes conducting capacity-building with governments and the private sector and supporting international measures intended to prevent illicit trade. Alpha tracks all known cases of illicit trade and the manufacturing base for proliferation-sensitive goods. The project also produces guidance on the implementation of non-proliferation controls, some of which has been adopted by the UN Security Council. For more information on Project Alpha, visit the Alpha website: www.acsss.info

Some technologies and items can be used both in normal industry and commerce as well as in nuclear weapons or missile programmes. These items and technologies are referred to as 'dual-use' and they present a significant weapons proliferation risk. Countries attempt to prevent these items from being diverted from peaceful uses to making weaponry by using national border controls and by establishing international mechanisms. But despite the adoption in 2004 of UN Security Council resolution (UNSCR) 1540, developed to counter this and other related challenges, illicit trade continues to fuel the proliferation of weapons of mass destruction. Nevertheless, the fulfilment of the call for full implementation of the resolution by 2021 has the potential to eliminate, or at least vastly reduce, the occurrence of such trade.

The reality is, however, that even if there were an effective system to monitor 1540's implementation, which there currently is not, the target of full implementation is likely to be missed. Worse still, because of a lack of effective metrics related to the resolution's implementation, the substantial yet limited resources available to support it cannot be effectively prioritised. Nonetheless, the work of Project Alpha, VERTIC and others shows that progress can be made to improve implementation of the resolution particularly with regards

In this issue

Trust & Verify
January-March 2015 • Issue Number 148 • ISSN 0966–9221

Verification Research, Training and Information Centre (VERTIC)
Development House
56–64 Leonard Street
London EC2A 4LT
United Kingdom
tel +44 (0)20 7065 0880
fax +44 (0)20 7065 0890
website www.vertic.org

to supply chain risks, which cannot be addressed by any one state alone. A key objective of the forthcoming comprehensive review in 2016 of resolution 1540's implementation, therefore, should be to find ways to work with civil society to further the aims of this important international instrument.

State-sponsored transfers of WMD, which have always been infrequent, have been in general decline since at least the 1970s. It can be argued that the measures taken by the US as a result of the so-called 'Indian Peaceful Nuclear Explosion' in 1974, including the talks that resulted in the formation of the Nuclear Suppliers Group, were instrumental in reducing such trade.

This reduction in supply has evidently not eliminated demand for WMD, however, and since the 1970s a number of countries have pursued these weapons by importing technologies illicitly from the international marketplace. While much attention is given to the AQ Khan network, and more recently to Iran's use of illicit procurement practises, illicit procurement that did not involve Khan's network has supported the nuclear and missile programmes of at least a half dozen countries, including Pakistan, Iraq, Iran, Libya and North Korea.

Unfortunately, efforts to prevent the illicit trade in dual-use technologies got off to a slow start. UK officials became aware of Pakistani procurements of high-frequency inverters in 1978, which, among other uses, are used to rotate uranium centrifuges. This occurred almost at the same time as the Nuclear Suppliers Group entered its decade-plus interregnum between meetings, meaning that there was no body through which to coordinate the adoption of measures to counter illicit trade in such dual-use goods.

It was not was not until the discovery of the extent of Iraq's clandestine nuclear program in the 1990s that the export control regimes began to adopt such measures. The discovery of the Khan network then resulted in the adoption of resolution 1540 in 2004 (according to interviews conducted by the author with practitioners who were involved in the resolution's drafting) which requires all states to take a variety of measures to prevent proliferation through illicit trade.

The resolution requires states to adopt a wide range of measures in order to combat illicit trade, but it is not necessarily clear which specific measures should be used. The mechanism used by the 1540 committee takes the form of a 'matrix', or set of 'matrices' (in effect a standardised questionnaire to be completed by UN officials in New York for every country), identifying some 26 measures in this area. However, a reading of the resolution highlights that over a third of these measures do not actually feature in the text of the resolution. Clearly states need to adopt and enforce an export control law which has appropriate punishments, and probably it is a good idea for the state to have an export licensing system in place, but is it necessary to control deemed exports—where an export is deemed to have taken place—if the knowledge or technology is transferred to a foreign national within the country?

There also appear to be omissions from the matrices that are implicit in the resolution. For example, the sharing and use of intelligence for enforcement and interdiction purposes is perhaps the main factor—after the adoption and enforcement of relevant laws—that can counter illicit trade but it is not listed in the matrices. Nor is interdiction (meaning measures to intercept goods during shipment); an omission that was necessary to secure Chinese acceptance of the resolution.

This discussion of what is in or out of scope of resolution 1540 is not irrelevant. When devising a methodology for export control capacity-building, the author attempted to work from the headings given in resolution 1540 to ensure that the capacity-building work being undertaken also aligned to the objectives of the resolution, but found limitations to this approach. Many of the measures required by the resolution are also inherently complex. For example, the resolution requires catchall controls and transhipment controls to be implemented. This requirement entails a complex interaction between intelligence, export control and customs officials, all of which must be underpinned by a legal basis and bureaucratic process.

Supporting implementation effectively: coordination is key

The complexity of the resolution's requirements is one of the main barriers to its implementation, with another being political commitment. It is to overcome this complexity that

a substantial community of 'donors' over the last decade provided hundreds of millions of dollars in capacity-building and assistance.

The capacity-building programmes of the US and EU are particularly significant due to their size. There are in fact, though, many 'donors' or assistance providers, including both individual states and civil society. The sheer number of donors and implementers raises the question of how best to coordinate these efforts to prevent a 'competition' among donors, which could overwhelm recipient states (many of which have limited human resources to devote to day to day implementation). In some states, for example, there are so few customs officials with knowledge of export controls that removing one from duty for the purposes of training can mean that there are no staff available to enforce the controls for that period.

It seems then that mechanisms are required that facilitate cooperation rather than competition in capacity-building assistance for resolution 1540, The 1540 committee and its group of experts has the potential to provide the basis of such a mechanism, but there are some practical challenges that must be overcome. The first is that there is a lack of understanding about how resolution 1540 is being implemented. The key question when examining national implementation should be whether the state has adequate measures in place to prevent involvement in proliferation, which is the goal of resolution 1540.

While much is made of the high reporting rate associated with resolution 1540, the reality is that most states' reports are inadequately detailed to answer the question set out above. This continued to be the case even after a template was introduced and is perhaps a result of 'reporting fatigue' in relation to UN resolutions.

States are required by the Security Council to report how they implement most UN sanctions resolutions as well as resolution 1540. For smaller UN missions and foreign ministries, it can be difficult to staff this requirement at all, let alone provide detailed answers to nuanced legalistic and enforcement questions.

For these reasons, the 1540 committee created its group of experts, whose main task is to monitor implementation of the resolution through its 1540 matrix process. This involves the experts, rather than the national governments, conducting a review of each country's implementation.

While the matrix process leads to a more uniform picture as to which of the resolution's requirements are being implemented in each country, there are numerous practical challenges associated with this assessment approach. For one, the matrices currently published are more than five years old, with the group of experts having missed its 2014 deadline to update them ahead of the 'comprehensive review' of resolution 1540's implementation, which will take place in 2016. They are now expected in mid-2015.

Another challenge is that while it may be relatively straightforward to identify whether the specific requirements of the resolution are implemented in national laws, it is much harder to gauge whether these laws are being effectively implemented or enforced. This challenge is compounded by the fact that the experts sit in New York and primarily conduct desk reviews (although several 'country visits' have recently been conducted, which provides an opportunity for the committee and group of experts to gain greater insight into how the resolution is being implemented).

An additional concern is that the matrices focus on implementation of the resolution's requirements and not upon the risks that the resolution was adopted to overcome. In the matrix process, it is not relevant if a country has a thriving industry producing dual-use items or if it is a common transhipment state: it only matters if laws exist and that they are being enforced, for example. These two limitations—the lack of a good metric for how the resolution is being implemented through laws and enforcement and a lack of understanding of the risks that individual states could inadvertently become involved in proliferation—mean that it is difficult or impossible to prioritise capacity-building efforts through the 1540 mechanism.

Proliferation threat

Resolution 1540 is evidently a means to an end. Yes, it requires states to adopt a range of specific measures. However, it is the bigger aim of preventing illicit trade that the Security Council was pursuing when it adopted the resolution.

A focus on proliferation would result in a greater effort to understand the manufacturing base of proliferation sensitive goods and on tracking trends in illicit trade. For a variety of reasons, the 1540 committee does not track either aspect. The author's experience suggests that governments (and by inference, the members of the export control regimes) also do not have a sufficient understanding of these matters. These are gaps that we at Project Alpha have sought to address. KCL research has mapped the manufacturing base and typical supply chain for some 20-plus 'chokepoint' technologies and has documented all known illicit procurements for Iran's nuclear programme.

Manufacturing base for dual-use technologies spreading, but slowly

The key findings of this work are that the manufacturing base for these technologies is not rapidly expanding as some may expect. In fact, it is generally only in China that systematic efforts to indigenise production of strategic technologies appear to be taking place under the country's '5 year plans'. It seems that for most of these technologies China is not yet capable of manufacturing to international standards and that, as a result, proliferators continue to be dependant on dual-use goods manufactured in the more traditional advanced industrial countries.

Take for example carbon fibre, which is is produced by only a handful of firms worldwide (fewer than 10, in fact). Composite materials including carbon fibre are targeted for indigenisation under the latest five year plan in China. More than 20 aspirant producers are working to turn this plan into a reality. These firms are capable of manufacturing significant quantities of the lower grade of the material but can manufacture little more than batch quantities in the kilogram range of the higher grade materials—the type needed for use in the production of centrifuges.

There are substantial barriers to the indigenisation of the production of controlled goods like carbon fibre, which indicate that this is unlikely to change in the near term. Such barriers include controls on production equipment like specialist industrial ovens, a limited availability of high-quality precursor material, and tacit production knowledge (know-how), which is particularly difficult to transfer.

Proliferators continue to use technologically-advanced states

The second major finding of this work is perhaps to be expected. It is from the most technologically-advanced states that proliferators seek dual-use goods. However, such countries also typically have in place relatively strong export controls meaning that goods tend not to be exported from these states directly to end-uses of concern. Instead, the risk is that goods proliferators will utilise illicit procurement methods to divert goods manufactured in advanced industrial countries—diversion that usually occurs in the supply chain.

A variety of techniques have been used by proliferators to achieve such diversion. In some cases, as detailed by Project Alpha, they have made efforts to disguise the true end use of goods. In other cases manufacturers or distributors and agents have been complicit. What is common among many of the cases is that the same third countries are utilised to tranship the goods. In this context, China again features as a particularly common transhipment point. Turkey also features prominently. The traditional transhipment points such as UAE and Malaysia also continue to feature, although perhaps less than they once did.

Proliferation evolving to take advantage of new methods for illicit trade

A final issue is that, since the adoption of resolution 1540, technological advancement has meant that the modalities of proliferation have begun to change. For example, the risk of internet trading platforms is one factor that is changing the nature of proliferation supply chains. Increasingly, it is possible for any individual to act as a distributor of sensitive goods by listing them on a site like Alibaba. Other factors include the advancement of cyber intrusion as a proliferation risk.

For example, data related to the Joint Strike Fighter (JSF) was stolen through cyber intrusion leading to speculation that Chinese hackers could be responsible and that the data could have been used in pursuit of China's own JSF-like plane.

Improving the impact of capacity-building

Given the challenges outlined above, what can be done to realise full implementation of the resolution? There appear

to be three main options: improved 1540 mechanisms, the use of other intergovernmental mechanisms, and civil society led actions.

1540's mechanisms: The 2016 comprehensive review of 1540's implementation provides an opportunity to reconsider what work is undertaken by the 1540 committee and its group of experts. The work of Project Alpha indicates that there are a variety of specific actions that the 1540 committee should take.

It should reinvigorate the 'request for assistance' mechanism to ensure that the status of requests is monitored even if implemented by a third party or a donor, rather than by the committee or group of experts itself. It should also continue to encourage states to adopt 'national action plans' as a mechanism through which the state itself can both identify gaps in its implementation of 1540 and plan how best to overcome the gap.

The 1540 committee should also review the terms of reference of the group of experts to ensure that the group focuses upon efforts that contribute to the resolution's ultimate objective of preventing illicit trade. This should include ensuring that the group of experts regularly maintains the matrices rather than updating them only after five years, as they are doing at present. A rolling system of assessment could easily be devised that would see all the matrices updated every 2-3 years.

Other Forums: In addition to the 1540 mechanisms, there are a variety of other international forums through which measures to overcome illicit trade can be coordinated. Perhaps most prominent among these are the international export control regimes, such as the Nuclear Suppliers Group. However, there are also other mechanisms, including the UN sanctions committees, and the Proliferation Security Initiative.

Perhaps the primary problem with these regimes is the lack of a information sharing apparatus to connect with states outside the regime. Although 1540's mechanisms cannot act as an intelligence-sharing forum, there is more information and guidance materials that they could distribute. The proliferation case studies and sectoral guidance produced by Project Alpha provide an example of the types of information (see below) that could usefully be shared in this way.

Civil society: Civil society is the often a forgotten and neglected actor in relation to improving the national implementation of resolution 1540, with the 1540 committee having thus far failed to devise effective ways to work with civil society.

Civil society is a key implementer for capacity-building efforts. In addition to conducting its own independent capacity-building and assistance activities, it is often civil society that implements programmes based on contributions from donors. There are good reasons for this: governments have limited resources to invest in capacity-building in third states. What trained staff do exist are needed to implement the state's own implementation activities.

Civil society organisations, for their part, are often staffed by former government officials and academic specialists, many of whom have developed experience and expertise in training and education. These skills are in addition to subject matter expertise, which is vital when conducting outreach.

Civil society can also access and leverage novel funding sources to engage in outreach activities—funding which is typically not available to states. For example, philanthropic trusts can and do provide funding that can be put to non-proliferation purposes. In order to fully utilise the resources available to civil society, it is nonetheless vital that implementation gaps and priorities are articulated.

Overcoming Supply Chain Issues

Improving the national implementation of 1540 is vital to prevent illicit nuclear trade. However, as set out above, while improvements to national implementation are central to achieving 1540's objectives, the issue of supply chain risks must also be addressed—issues which are transnational instead of national in scope meaning that they cannot be addressed by stronger implementation of controls in any one state or group of states alone.

More effective coordination and cooperation across jurisdictions can go some way to counter this risk (in particular with

regards to intelligence and interdiction operations, which as explored above may be considered outside of the scope of resolution 1540), but research at KCL has highlighted the need to also work with the private sector to counter such supply chain risks.

This transnational aspect of supply chains makes private sector engagement particularly challenging. Project Alpha has sought to address these challenges head on. In 2011, a discussion paper entitled 'Antiproliferation: Tackling Proliferation by Engaging the Private Sector' was published. Since then, Alpha has conducted extensive sectoral engagement. This work has culminated in a number of sectoral guides on the implementation of trade controls.

In order to address the transnational aspects of supply chains, KCL has also worked with international bodies and groups to promote the adoption of such guidelines internationally. This has included securing support of members of the NSG to publish guidelines on 'Good Practices for Corporate Standards to Support the Efforts of the International Community in the Non-Proliferation of Weapons of Mass Destruction'. Working with the governments of Australia and Singapore Project Alpha also produced guidelines for the maritime transport sector on compliance with UN sanctions that have since been published by the UN Security Council. Finally, a guide on implementation of export controls in universities is to be submitted by the UK government to the 1540 committee as an example of an 'effective practice'.

Measures like these go some way towards setting global standards to counter supply chain proliferation risks. However, further work is evidently needed in this area. In particular, it would be beneficial to bring together firms from each sector in order to socialise the standards and begin to build a nonproliferation culture. Without taking such measures, it is unclear whether the transnational nature of illicit trade through the supply chain can be addressed.

Conclusion

Despite progress in countering state-sponsored transfers in support of weapons program, proliferation continues today much as it has for the last three decades: proliferators are acquiring dual use goods and materials or the equipment for their manufacture illicitly from the international marketplace.

Measures to counter proliferation, including the adoption of dual-use export controls and the adoption of resolution 1540, go some way toward creating a landscape that could counter illicit trade. The truth is, however, that the current levels of coverage and implementation of export controls continues to undermine their effectiveness. Worse still, there continues to be a lack of understanding about how controls are being implemented at the national level. Gaining a better understanding of how these measures are being implemented would allow for better prioritisation of capacity building efforts.

Ultimately, to truly counter illicit trade, national implementation of 1540 will need to complemented by a consideration of how best to secure supply chains on a global basis. Such activity is vital, ultimately, as proliferators are dynamic and will continue to evolve their approaches in pursuit of their proliferation goals. The 2016 comprehensive review of 1540's implementation will provide an opportunity to discuss how best to engage civil society, which has resources and experience to bring to bear, in this effort. •

Ian J. Stewart
Head, Project Alpha, King's College London

Verification Watch

Sentencing of toxin salesman from the dark web

Yasemin Balci and Russell Moul, London

The previous issue of *Trust & Verify* (no. 147) featured the case of Ms Kuntal Patel who was sentenced in November 2014 in the UK for three years for buying the toxin abrin 'without a peaceful purpose'. This is a crime under the UK Biological Weapons Act, the law which implements the 1972 Biological Weapons Convention (BWC) in the UK. Ms Patel purchased the abrin from a US resident named Jesse Korff. He was also caught and prosecuted for his criminal acts, then sentenced this February for violating the US Biological Weapons Anti-Terrorism Act, which implements the BWC in the US.

Mr Korff operated through an illicit website on the dark web, an area of the internet that is not indexed by standard search engines. The website, known as 'Black Market Reloaded' (BMR) offered goods that included biological agents, toxins, chemicals, firearms, ammunition, explosives, narcotics and counterfeit products. From August 2013 to January 2014, Mr Korff not only advertised the sale of these toxins but also offered potential customers information on the dose needed to kill individuals of given weights, as well as instructions on administering the toxins. Mr Korff would also claim that murders carried out in this fashion would go undetected, as symptoms would be similar to those caused by a bad case of flu. By the time he was arrested on 18 January 2014, Mr Korff had sold the toxins ricin and abrin to international customers in India, Austria, Denmark–and to Ms Patel in London.

The arrest took place just before he was able to ship a second dose of abrin to Ms Patel who, after panicking, had disposed of the first batch. An undercover federal agent purchased abrin from Mr Korff on BMR, which, Mr Korff said, would be hidden in a candle (the same process he used to send abrin to Ms Patel). After his arrest, the FBI searched his property and recovered a vial of abrin that Mr Korff was preparing to ship to London, which triggered the UK authorities to investigate Ms Patel. They also recovered computers as well as the plant seeds from which ricin and abrin can be extracted; the commonplace castor bean (a seed from the ricinus communis plant) and rosary pea (a seed form the abrus precatorius plant).

Castor beans are processed throughout the world to make castor oil, which is commonly used in medicine as a laxative or as a preservative in the food industry. Ricin is part of the waste 'mash' that is produced when castor oil is made. The abrus precatorius plant is for its part completely toxic, but the highest concentration can be found in its seeds. Ricin and abrin are thought to affect the body in similar ways–they inhibit protein synthesis, which leads to cell death. Symptoms manifest in different ways depending on the route of exposure. If ingested, the victim will experience severe abdominal pain, vomiting and diarrhoea, which can lead to organ failure and death within a few days.

Following his arrest, Mr Korff was sentenced to imprisonment for nine years and two months and a $1,000 fine after he pleaded guilty to, among other charges, five counts relating to biological weapons in violation of Section 175(a) of Title 18 of the US Code (the legal instrument that organises and consolidates the main laws of the US, including the US Biological Weapons Anti-Terrorism Act). Section 175 (a) of the Title prohibits anyone from knowingly developing, producing, stockpiling, transferring, acquiring, retaining, or possessing any biological agent, toxin, or delivery system for use as a weapon. 'For use as a weapon' means any activity with biological agents or toxins that does not serve a peaceful purpose. 'Toxin' is defined in Section 178 (2) of the same Title as 'toxic material or product of plants, animals, microorganisms […] or infectious substances, or a recombinant or synthesized molecule, whatever their origin and method of production'.

In the US, particularly dangerous toxins such as ricin and abrin also feature on the 'select agents and toxins' list and are thereby subject to governmental control in terms of their possession and handling. This is in line with the BWC, which requires states parties to take measures to not only 'prohibit', but also 'prevent' any activities involving biological weapons. •

Cyber war games: a new tool for cyber security

Katherine Tajer, London

In January, British Prime Minister David Cameron and US President Barack Obama announced a bilateral effort to increase the ability of the UK and US to respond to cyber attacks. The two countries will begin exercises later in the year—dubbed as 'cyber war games' by the mainstream media—to identify limitations and vulnerabilities within their cyber defence and resilience infrastructures. The games will involve simulated attacks targeting the two states' financial hubs: the City of London and Wall Street.

In order to create a realistic attack scenario, participants will manage and protect their systems while also attempting to infiltrate and damage their opponents' networks. President Obama confirmed his commitment to cyber security in the January 2015 State of the Union Address, calling for legislation to grant further cyber protections for US citizens. The last few months have seen several announcements by the US government regarding plans to upgrade their agencies' and military cyber defence capabilities. The timing of these efforts is not a surprise, given several recent high-profile cyber incidents. The most prominent of these, allegedly orchestrated by a North Korean group called the 'Guardians of Peace', resulted in the release of a large amount of internal Sony documents.

Private companies within the financial sector have been running intra-sectoral simulations since at least 2011. In the UK, 'Waking Shark' was staged as a tabletop exercise for the finance industry in 2011. Since then, the Securities Industry and Financial Markets Association (SIFMA), has sought to address cyber concerns within the private sector by organising multi-national exercises as well. Organised by the consulting group Deloitte and Touche, SIFMA hosted 'Quantum Dawn 2', which simulated attacks that directly affect market performance such as stealing administrator credentials to fraudulently sell stock. Deloitte and Touche reported that the simulation successfully shared protocols and 'identified areas where the industry can improve its crisis management procedures and strengthen relationships among the industry participants.'

Since 2010, countries have been collaborating in multilateral exercises to respond to a range of types of cyber attacks including some with wider national security implications. NATO, for instance, has conducted four extensive multilateral exercises since 2010. NATO's exercises are designed to accurately imitate a state-to-state or third-party-to-state attack, aiming to replicate potential physical destruction rather than economic impairment. The first attempt, called 'Baltic Cyber Shield', tested six teams representing private, public and academic expertise in Sweden, Latvia and Lithuania. Baltic Cyber shield focused specifically on vulnerabilities in 'supervisory control and data acquisition', or SCADA systems, which are computer-based large-scale industrial control systems. Targeting simulated steam engines, models of solar power plants and power distribution grids, the exercise sought to imitate incidents like the Stuxnet attack on Iranian centrifuges.

Since then, NATO has run three further cyber defence exercises, the most recent of which involved over 28 countries and 670 participants. The participants were divided into responder and attacker teams. The responder teams competed with one another to see who dealt best with the attacks while managing media output regarding the simulated incident.

These exercises use a 'white-box' approach, meaning that the attacker teams were given comprehensive details about a target's online environment including information about potential vulnerabilities. This approach was taken because real-life hackers can effectively set their own timetable to observe and understand an online environment before developing an attack. By giving the attackers this information from the start, they were able to carry out a skilled cyber attack quickly, and successfully emulate an advanced threat.

Several national simulation programmes are designed to be flexible enough that they can apply to both private sector and national security concerns. The US government has carried out a variety of cyber simulations through the Department of Homeland Security and through the creation of the Idaho National Laboratory's cyber security 'test bed'. The test bed can recreate a precise environment for the user's needs and then run simulated attacks to isolate vulner-

abilities or prepare for specific scenarios. The test bed is capable of testing SCADA and critical infrastructure vulnerabilities—both major concerns for governments. The Brazilian army has for its part developed a similar piece of equipment to train cyber defence teams. Like the US technology, this equipment can be manipulated to simulate attacks against civilian or military targets.

Real-life cyber attacks can provide many lessons for strengthening cyber security among concerned stakeholders, but lessons must be disseminated to be learned. Historically, companies have been resistant to share this information because it could reveal that they have inadequate cyber infrastructure and potentially damage their reputation. Efforts to increase information-sharing within the private sector and impose laws to compel private companies to share data on cyber threats and tactics are ongoing within the US and UK. Simulations, alternatively, offer a method to share best practices without revealing internal weaknesses.

There are many apparent technical advantages to war games compared with tabletop exercises, or even information-sharing after actual attacks. For one, participants look for evidence of an attack from the beginning of play. This allows for observation by the affected team from the start of the attack which teaches security professionals to recognise infiltration early on. During an actual attack, the victim may not notice any changes in the environment until it is too late. If executed well, an interactive cyber exercise can allow states and private companies to demonstrate best practices as well as identify gaps and challenges in the field. Furthermore, the basic cyber war game format can be adjusted easily to incorporate new forms of technology. Frequent games are necessary to stay abreast of developments within cyber warfare.

Another benefit to games is that security professionals can be put in the seat of the hacker. Symantec, an American IT security firm, has run an annual simulation called 'CyberWar Games' for the last four years. All of their employees are invited to form teams of hackers and to attempt to infiltrate a specific set of data: last year, for example, they attempted to hack into a fictional hospital's health records. Symantec employees have stated that this type of exercise has allowed them to think about different areas of focus when carrying out audits and securing networks—essential processes within security.

Those involved in maintaining national security may see diplomatic advantages in running effective multilateral simulations since they provide opportunities for states to coordinate on cyber capabilities and resilience, and demonstrate a public commitment to security concerns beyond what many would consider as traditional international security alignments. In the spring of 2014, the International Cyber Shield Exercise provided the widest cross-alliance exercise to date, involving 19 countries. Hosted in Istanbul, the exercise included Albania, China, Malaysia, Turkey and Iran, among others. The low stakes, non-binding nature of the exercises means that states can share initiatives with relatively few consequences. Increasingly over the last five years, NATO's exercises also involved teams to develop fictional legislation to help states better coordinate and recover, which perhaps could later be expanded and applied internationally.

While there has not been a large amount of criticism of cyber simulations to date, those who have spoken against them, from a technical and procedural perspective, have argued that the games are too bureaucratic in nature. The desire for some of these games to involve a large number of representatives often causes these exercises to become bureaucratic and inflexible. Recommendations for improvement include the creation of multilateral exercises between agencies—already underway as the US and UK embark on a game joining MI5 and the FBI.

One potentially disturbing feature of the growth of cyber war games is that it indicates that cyber space is becoming a more accepted arena for physical and economic cyber attacks. On the other hand, these simulations could be used to provide an informed starting point for the development of international norms and agreements. Given the current ambiguity over the nature and consequences of cyber attacks, and the heightened rhetoric over cyber threats to national security, proactive measures such as these may be preferable to a 'wait and see' approach. •

Cyber attacks: the challenge of attribution

Alberto Muti and Cervando Banuelos II, London

In February 2015, cyber security firm Kaspersky Lab announced they had discovered a highly advanced and secretive outfit they called the 'Equation Group' that specialises in espionage and the collection of information through cyber infiltration. Kaspersky Lab documented roughly 500 infected machines globally.

However, traces suggest that the group has been active for at least 14 years, and the total number of infections might be as high as 10,000 . In their report, Kaspersky Lab claim to have found evidence of a connection between the Equation Group and the authors of the attacks known as Stuxnet and Flame, which were allegedly developed by US agents under the codename 'Operation Olympic Games'. The claim is based on similarities between the code and methods of attacks used.

The alarm raised over the activities of the Equation Group reminds us that highly sophisticated cyber attacks are not a potential future risk but are already part of daily reality. However, efforts at the international level to find ways of curtailing cyber attacks have lagged behind the threat, often hindered by profound disagreements between states and among citizens on the societal function of the internet in the modern world and what the role of the government should be in cyber space. Proposals by international organisations, such as the UN and the EU, stress that the internet should remain a safe space for individuals and economic activities.

These, however, have been limited, for the time being, to broad statements lacking means of concrete application. The first step in developing agreed international norms for cyber space is achieving a common understanding on what constitutes a particular type of cyber attack and what kind of response it should entail. The strengthening of any such norms would likely require an agreed process for identifying whether a certain type of attack took place and who did it. This underlines a key issue in cyber security: the attribution of cyber attacks.

Attribution—the process by which the perpetrator of an attack is identified—has long been an important issue in technical debates on cyber security. Current attribution techniques rely heavily on the initial collection and processing of data regarding the attack. Containing and quarantining contaminated files and data for study is typically the first step. Once the data is collected, it is important to maintain its 'compromised integrity': if the infected data is erased or repaired, such as with software updates and security patches/scans, any traces the attack left behind could be lost. In the event of an ongoing attack, the collection of live system data is crucial to understand what malicious code is doing to a network. If data has been erased by malware during an attack it can sometimes be recovered, and their analysis can help study the attacker's strategy, and provide a launch-point for attribution.

A common approach in attempts to trace attacks back to the perpetrators consists of systematically logging all the traffic that went through the network and 'querying', or analysing, the logs looking for specific markers in information transmitted through the network. These markers can be specific e-mail addresses, attachments, or other information that says where the message came from. Ideally, these markers can be used to trace a path back to the attack's point of origin. Investigators can also use 'offensive' attribution techniques, aiming to exploit the attacker. For example, it is possible to set up a 'honeypot' network that is purposefully vulnerable, in order to lure attackers into revealing their attack patterns. It is also possible to directly 'attack back' during ongoing attacks and attempt to extract information from the attacker. These techniques allow investigators to exploit an attacker's actions directly to gain valuable data. A downside of this approach is that if attackers become aware of these actions they can obfuscate their tracks or purposefully provide faulty information on the attack.

The investigation into the Equation Group's activities is an example of a complex attribution process. The attack used several different pieces of malicious software, working in coordination to infiltrate a target. These programmes reported back to a network of 300 'command and control' (C&C) servers, through which the group received information on their targets and controlled the implanted software. Reportedly, a key mistake made by the attackers was that the lease for approximately 20 of these servers had expired.

Kaspersky Lab discovered the C&C network by querying traffic from infected computers. Upon realising that some of these servers were not under the attackers' control anymore, the investigators bought them, and used them to collect and analyse the information sent by the malware. This operation was difficult to carry out, and would have been even more so had the attackers not allowed the lease on their C&C servers to expire. In this instance, however, it allowed Kaspersky Lab to establish with confidence that the different pieces of malware were part of a complex, coordinated attack. It is worth noting again that, while the investigation managed to reconstruct the attack's very complex strategy, and to find clues connecting the Equation Group to other cases, it has not managed to provide a precise fix on the perpetrator's identity and location.

Ideally, the attribution of any cyber attack would identify the perpetrator with high confidence, but this is not an easy task. The challenges in attribution are defined by the limitations of the technology used to trace attacks back from the victim to the point of origin: even if a route to an attacker is traced, this kind of information can be obscured in order to hide the identity of the perpetrator, or even falsified to incriminate others. Many practitioners appear to maintain that in the case of a sophisticated attack, a complete traceback to the original source through cyber means alone – that is, without the use of other forms of intelligence or investigation—is almost always impossible.

Current methods can help trace attacks back to certain geographic regions and internet service providers (ISP), but often come short of identifying the precise point of origin. This can requires cooperation from the ISP, which is not always easy to secure, as these are often located in other countries and operating under different jurisdictions to a victim.

These constraints could potentially be mitigated somewhat through forms of political cooperation at the international level. From this point of view, it can be useful to look at attribution as a form of verification. More specifically, it can be seen as a form of post-hoc verification, which is carried out when there is the suspicion that proscribed activities have taken place. The verification perspective can help identify key issues of relevance when talking about the attribution of cyber attacks. For example, it is important to have an understanding of what the purpose of the verification process is. It may be an assessment of whether a prohibited attack has taken place. Alternatively, it might entail collection of evidence aimed at establishing the identity of the perpetrator. Or it could attempt to achieve both objectives.

Another key question regarding verification is the reliability of the processes and techniques employed, and the level of accuracy and confidence expected in the result. Any method of investigation has its own strengths and weaknesses, and produces differing levels and types of confidence. This is especially relevant given the current limitations of cyber attribution techniques.

However, the arms control sector can offer examples where verification systems have been established despite acute technical or political challenges, or both. This typically involves work to frame the scope of the system and the targets of verification, who should be involved, and how it should be carried out. At the moment, disagreements in the international community have stymied progress on international arrangements guiding or governing the use of cyber attacks. However, even limited forms of international cooperation would help to clarify, and potentially calm, interactions between states. •

Programme News

Verification and Monitoring Programme

Over the past three months, work has continued on the VM programmes' main projects on multilateral verification of nuclear disarmament and universalisation of the IAEA Additional Protocol. In January, VM team members Larry MacFaul, David Cliff, Hugh Chalmers and Alberto Muti travelled to Yaoundé, Cameroon, to hold a workshop for Cameroonian government officials on safeguards and the Additional Protocol. This is the fourth such workshop that VERTIC has held in Africa since this project began. Work on surveying country legislation, which forms the backbone of this project, has meanwhile continued.

On the other main VM front, multilateral verification of nuclear disarmament, the past quarter has seen the organisation and hosting of the sixth and final meeting of the international experts that VERTIC has assembled to steer and review implementation of this project. On this occasion the group met in London, where all VM team members presented. Main topics of discussion including ongoing VERTIC work to develop notional nuclear fuel cycles and disarmament scenarios for trialling verification methodologies, forthcoming VERTIC publications and a review of political developments relating to the work. This project is now in the final part of this first phase.

We are pleased that this quarter has given us the opportunity to continue our work through the renewal of a nu,ber of important grants. The VM team recently heard that bids to continue work on strengthening implementation of IAEA safeguards and facilitating ratification of the Additional Protocol.

In addition, we have had success in applying for the restart of VERTIC's project of engagement with Chinese arms control NGOs, designed to bring together scholars from the UK with those in China. The pilot phase of this project was completed in January this year. Work to launch the second phase of the China project is already underway. •

National Implementation Programme

During this quarter, the NIM team remotely reviewed a draft bill implementing the Chemical Weapons Convention (CWC) and Biological Weapons Convention (BWC) for a Latin American state. Legal Officer Sonia Drobysz also published an article on 'Safeguards and Verification' in a research brief by the International Network of Emerging Nuclear Specialists, on the strengthening of Article X of the Non-Proliferation Treaty (NPT), which relates to the issue of withdrawal from the NPT.

From 12-13 January, Sonia Drobysz gave a presentation during an awareness-raising workshop on the BWC and United Nations Security Council Resolution 1540 (UNSCR 1540) in Cotonou, Benin. Senior Legal Officer Yasemin Balci joined her from 14-16 January for a legislative drafting workshop with Beninese officials.

Sonia Drobysz and Yasemin Balci then travelled to Kampala, Uganda, to review the Uganda Biosecurity Bill with relevant governmental stakeholders from 19-20 January. From 28-30 January, Sonia Drobysz and Yasemin Balci worked with officials from Burkina Faso in Ouagadougou on their first draft of a bill implementing the BWC. All of these workshops formed part of the European Union's BWC's Action programmes for Benin, Burkina Faso and Uganda.

From 2-6 March, Yasemin Balci participated in a regional workshop on 'Security, the Implementation of the CWC, and Cooperative Threat Reduction in Africa', organised by the African Union, United States Department of Defense's Threat Reduction Agency and the Organisation for the Prohibition of Chemical Weapons. Ms Balci presented on national implementation of the CWC and UNSCR 1540 in the national legal order.

From 23-24 March, Sonia Drobysz participated in a regional workshop on 'Implementation of Resolution 1540 (2004) in the Caribbean', organized in Lima, Peru, by UNLIREC, the UN Regional Centre for Peace, Disarmament and Development in Latin America and the Caribbean. She presented on various approaches to adopting national implementation measures for UNSCR 1540. On the same two

days, Programme Director Scott Spence participated in the 2015 Carnegie International Nuclear Policy Conference in Washington D.C., United States. He also attended an event at the Palais des Nations in Geneva, Switzerland on 30 March to mark the 40th anniversary of the entry into force of the BWC. •

Publications News

Contribution on safeguards to INENS research brief

NIM legal officer Sonia Drobysz recently contributed a chapter on 'Safeguards and Verification' to a research brief on 'Developing Consensus on Strengthening Article X(1) of the NPT' published in January by the International Network of Emerging Nuclear Specialists (INENS). The brief provides a background of the issues relating to Article X of the NPT—which addresses the procedures and responsibilities associated with the exercise of the right of withdrawal from the treaty.

Ms Drobysz's chapter examines the types of safeguards-related measures that could be implemented upon announcement by a state of its withdrawal from the NPT as well as after it has withdrawn. 'Both during and after notice of the exercise of the right to withdraw from the NPT, IAEA safeguards should be continuously applied in order to verify the peaceful nature of material and equipment acquired and/or developed prior to withdrawal,' Ms Drobysz writes. 'Procedures aimed at consolidating the consequences of withdrawal should reaffirm and clarify the applicable safeguards legal framework, including the NPT, safeguards agreements (both comprehensive and item-specific), the IAEA Statute, relevant bilateral cooperation agreements, the [Vienna Convention on the Law of Treaties] and the UN Charter. The institutional framework and the role of all the actors involved, especially the IAEA Secretariat, the IAEA Board of Governors, the UN Security Council and NPT States Parties should also be clearly determined.'

INENS has been discussing the brief with government officials with a view to help build consensus on withdrawal at the 2015 NPT review conference. •

Verification Quotes

The main weakness of the BWC lies: where? It lies in the area of reassurance. That is the perennial gap at the heart of the BWC. It flows from the failure of the States Parties, building on the text as it stands, to derive a common understanding as to how to reassure one another and demonstrate that their shared commitment to biological disarmament governs what they are doing and what they allow to be done. Without it, doubts and suspicions persist and erode the credibility of the Convention as they stay unresolved. Nicholas Sims, speaking at the 40th Anniversary Event for the Biological Weapons Convention, Geneva, 30 March 2015.

For far too long, the international community has shied away from the responsibility of confronting the verification challenges that come with disarmament. For far too long, we have talked about multilateral disarmament without developing the tools that will actually get us there. Today, you are taking action. Rt Hon Lord Browne of Ladyton, speaking at the kick-off meeting for the US-NTI disarmament verification initiative, Washington DC, 19 March 2015.

Over the next month or so we're going to be able to determine whether or not their system is able to accept what would be an extraordinarily reasonable deal, if, in fact, as they say, they are only interested in peaceful nuclear programs. And if we have unprecedented transparency in that system, if we are able to verify that, in fact, they are not developing weapons systems, then there's a deal to be had. But that's going to require them to accept the kind of verification and constraints on their program that so far, at least, they have not been willing to say yes to. US President Barack Obama, speaking about the prospects for a long-sought deal addressing the Iranian nuclear programme, 8 March 2015.

Grants and administration

Cervando Banuelos II has joined the Verification and Monitoring Programme as an intern in February. He is in his final semester of a Master's programme at the Monterey Institute for International Studies. Programme Director David Keir has moved to Norway where he will continue his work for VERTIC. Angela Woodward will return from maternity leave in the next quarter. She served as the Programme Director of National Implementation from 2009 to 2014, and will now take up a new post as Deputy Director. We look forward to welcoming her back in this new capacity.

During the quarter, the UK Foreign and Commonwealth Office approved continuation funding for our projects on 'Strengthening implementation of IAEA safeguards and facilitating ratification of the Additional Protocol' and on 'Legislative assistance to counter the proliferation of CBRN weapons and related materials'. VERTIC also received funding to continue a project to foster an ongoing technical dialogue between UK- and China-based arms control scholars. We are grateful for these renewed commitments to our work on these issues. In addition, we have received funding from the Rufford Foundation to carry out in work on sustainable development. Joy Hyvarainen, a member of our International Verification Consultants Network and a former VERTIC Trustee, will carry out the project together with Andreas Persbo and Larry MacFaul. •

building trust through verification

VERTIC
Development House
56–64 Leonard Street
London EC2A 4LT
United Kingdom

tel +44 (0)20 7065 0880
fax +44 (0)20 7065 0890
website www.vertic.org

Registered company no. 3616935

Registered charity no. 1073051

VERTIC is an independent, not-for-profit non-governmental organisation. Our mission is to support the development, implementation and effectiveness of international agreements and related regional and national initiatives, with particular attention to issues of monitoring, review, legislation and verification. We conduct research, analysis and provide expert advice and information to governments and other stakeholders. We also provide support through capacity building, training, legislative assistance and cooperation.

PERSONNEL Mr Andreas Persbo, *Executive Director*; Ms Angela Woodward, *Deputy Director*; Dr David Keir, *Programme Director*; Mr Scott Spence, *Programme Director*; Mr Larry MacFaul, *Senior Researcher, Editor-In-Chief for VERTIC publications*; Ms Yasemin Balci, *Legal Officer*; Mr David Cliff, *Researcher*; Dr Sonia Drobysz, *Legal Officer;* Mr Hugh Chalmers, *Researcher*; Ms Katherine Tajer, *Administrator/Research Assistant*; Mr Russell Moul, *Researcher*; Mr Alberto Muti, *Researcher*; Dr Miguel Sousa Ferro, *Volunteer Consultant* (2014-2015); Mr Cervando Banuelos II, *Intern* (February-May 2015).

BOARD OF DIRECTORS Mr Peter Alvey; Gen. Sir. Hugh Beach; Dr Wyn Bowen; Rt Hon Lord Browne of Ladyton; Mr Oliver Colvile MP; Dr Owen Greene; Mr Sverre Lodgaard; Dr Edwina Moreton; Mr Nicholas A. Sims.

INTERNATIONAL VERIFICATION CONSULTANTS NETWORK Dr Nomi Bar-Yaacov; Ambassador Richard Butler; Mr John Carlson; Ms Joy Hyvarinen; Dr Edward Ifft; Dr Odette Jankowitsch-Prevor; Mr Robert Kelley; Dr Patricia Lewis; Dr Robert J. Matthews; Professor Colin McInnes; Professor Graham Pearson; Dr Arian L. Pregenzer; Dr Rosalind Reeve; Dr Neil Selby; Minister Victor S. Slipchenko; Dr David Wolfe.

CURRENT FUNDERS Joseph Rowntree Charitable Trust; Carnegie Corporation of New York; Department of Foreign Affairs, Trade and Development Canada; Norwegian Ministry of Foreign Affairs; Rufford Foundation; UK Foreign and Commonwealth Office; US Department of State; United Nations Interregional Crime and Justice Research Institute.

TRUST & VERIFY is published four times a year. Unless otherwise stated, views expressed herein are the responsibility of the author and do not necessarily reflect those of VERTIC and/or its staff. Material from *Trust & Verify* may be reproduced, although acknowledgement is requested where appropriate.

EDITOR Larry MacFaul
DESIGN Richard Jones
PRODUCTION David Cliff

SUBSCRIPTION *Trust & Verify* is a free publication. To subscribe, please enter your e-mail address in the subscription request box on the VERTIC website. Subscriptions can also be requested by contacting Katherine Tajer at: katherine.tajer@vertic.org