



## The RUSI Journal

ISSN: 0307-1847 (Print) 1744-0378 (Online) Journal homepage: <http://www.tandfonline.com/loi/rusi20>

# OMG Cyber!

Robert M Lee & Thomas Rid

To cite this article: Robert M Lee & Thomas Rid (2014) OMG Cyber!, The RUSI Journal, 159:5, 4-12, DOI: [10.1080/03071847.2014.969932](https://doi.org/10.1080/03071847.2014.969932)

To link to this article: <http://dx.doi.org/10.1080/03071847.2014.969932>



Published online: 04 Nov 2014.



Submit your article to this journal [↗](#)



Article views: 18354



View related articles [↗](#)



View Crossmark data [↗](#)

## COMMENT

## OMG CYBER!

## THIRTEEN REASONS WHY HYPE MAKES FOR BAD POLICY

ROBERT M LEE AND THOMAS RID

**For many austerity-hit Western countries, the defence budget has been a prime target for significant cuts. Nowhere has this been more apparent than in the United States. Yet one element of the Pentagon's budget continues to grow: cyber. High-profile security breaches at the corporate level and reports of cyber-espionage at the national level seemingly justify the vast sums involved in ensuring cyber-security. However, Robert M Lee and Thomas Rid argue that 'cyber-angst' is damaging – and self-serving. In this article, they list thirteen reasons why such cyber-security hype is counterproductive.**

Cyber is piping hot – and now more so than ever, with several scary precedents being set over the course of the last year. In late 2013, a massive security breach at Target, a major American retailer, compromised the credit-card data of as many as 40 million customers. A few months later, in May 2014, eBay suffered an even bigger breach that affected 145 million accounts. In September, intruders stole 56 million customer credit-card numbers from Home Depot, a US home-improvement chain. Also in 2014, in another first, the US Department of Justice indicted five serving members of China's People's Liberation Army (PLA) for stealing industrial secrets from several companies based in the Western District of Pennsylvania. Meanwhile, Eastern European criminal syndicates are busier than ever; 'Cybercrime is anonymous, sophisticated, and international – and Russian', says Lee Miles, deputy head of the UK's National Cyber Crime Unit.<sup>1</sup> In 2014, the market for information-security spending topped \$70 billion.<sup>2</sup> In September, NATO agreed

that a cyber-attack could trigger a military response.

In the US, all of this nurtures hype; and the Washington Beltway forms the ideal Petri dish in which to cultivate the alarmism – several parties think that overstating 'cyber' is in their own best interest. Security firms like a clearly stated threat in order to sell their security products. Contractors capitalise on fear to get funding from the executive branch. The Pentagon finds a bit of hype useful to keep the money coming in. The armed services each eye a larger slice of the budget pie. The White House loves some good cyber-angst to nudge law-makers into action. Fear of Chinese cyber-attack makes it easier for members of Congress to relate to voters. Reporting cyber-war means that journalists sell more copy. Academics get quotations and attention from the buzz. Hype up cyber, and everybody wins.

However, the real question is whether ramping up the threat of cyber-attack is really in everybody's interest. There are downsides to this dynamic. This article argues that cyber is 'hyped

out'. Overstating the threat does not just have benefits (for some): it also comes with significant costs. The benefits are short-lived and easy to spot, whereas the costs are long-term and harder to understand – and they are piling up fast and high. Indeed, they are so high that the debate inches towards a turning point *for all parties involved*. Here are thirteen reasons why a more nuanced debate is needed.

### One: Hype Creates Confusion

The US Department of Defense (DoD) has led the charge on militarising cyberspace. It has rung the alarm on cyber-threats and it does so as one of the most powerful organisations on the planet. The DoD is huge: it comprises around 3.2 million personnel in total with an annual budget of approximately \$500 billion. This includes the US Army, Navy, Air Force and Marine Corps, a vast civilian bureaucracy, more than a dozen defence agencies, the joint combatant commands and national-level intelligence services, such as the National Security Agency (NSA). With so



In the film *War Games* (1983), a teenage hacker accidentally tricks Joshua – a computer that controls the US nuclear arsenal – into playing war. Image courtesy of Everett Collection/REX.

many people and organisations under its umbrella, budgets are bound to be messy and controversial. Yet investment in cyber stands out.

The DoD's overall budget is shrinking fast; upwards of 100,000 personnel are expected to be cut as the Pentagon reduces the budget by more than \$75 billion over the next two years.<sup>3</sup> Budget cuts and an uncertain fiscal climate have led to the scrapping of programmes, capabilities and even entire agencies. Yet the cyber budget is growing. As revealed by the 2015 annual budget report, cyber-security is one of the few areas receiving more funding, not less – for research, defensive and offensive operations, and acquisition – mostly tied to US Cyber Command and the NSA. This has created a climate in which it is beneficial to have a tie-in to cyber. Programme managers know that if a budget could land on the chopping board, relabelling it as – or intertwining it with – 'cyber-something' could save it. Everybody uses computers, after all, and everybody wants them to be safe.

A bloated concept of 'cyber' – especially when used as a catch-all noun – means that it is ever-harder to say when something clearly *is not* cyber-

related. This is a problem that Robert Hale, a former DoD comptroller who stepped down in June 2014, understood all too well. When commenting on the 2015 budget, he stated: 'we tried to capture it all, but I'd say there's a gray area here in what counts as cyber'.<sup>4</sup> Leaders in government often lack technical expertise. Without that expertise it becomes difficult to sift fact from hype and core capabilities from creative costing: 'cyber' is now the Pentagon's 'pork', to put it in Congressional jargon.

## Two: Hype Limits Results

Organisations and their staff care about results. Organisations that do not produce results lose budgets, staff and missions, or even face being shut down. The DoD is under pressure to provide intelligence capabilities and defence options to the White House in a field short on skill. The result is that the Pentagon simply outsources many of its problems to the private sector. Companies are quick to offer highly priced cyber-expertise. The exact amount that the DoD is spending on contracts for cyber-security is unknown. However, Freedom of Information Act documents and the

large contracts being awarded suggest that the figure is in the billions of dollars.<sup>5</sup> A single cyber-security related contract awarded to Lockheed Martin in 2012 for 'technical, functional, and managerial support' was worth \$454 million.<sup>6</sup>

Relying on the private sector is nothing new and can be a good thing. The Pentagon alone could not create weapon system platforms such as the F-22, for example. Government contracts provide an opportunity to fill knowledge gaps on a temporary basis. However, the DoD has not limited its outsourcing *vis-à-vis* cyber-security to capabilities and temporary assistance. Large investments in purchasing technical support and hiring contractors to fill cyber-operations jobs come with a side effect: the government does not need to develop, train and maintain its own skilled cyber-professionals. On the world's conventional battlefields, using private military companies is highly controversial; in cyber-security, hackers-for-hire are the norm. Assessment cannot be outsourced, however, and a dearth of home-grown talent makes assessing results harder. Without skilled and tech-savvy professionals rising to the top on the inside of government, leaders will find it difficult to assess if an investment can return the desired results. Hype values input over output.

## Three: Hype Betrays Purpose

To achieve results organisations must have clear objectives; but cyber-hype means that organisations lose focus and purpose. As an example, the US military is making promises regarding cyber-operations that it cannot deliver upon. In 2006, the US Air Force (USAF) boasted that it would now 'fly, fight, and win in cyberspace'; in 2014, after eight years of multiple, ongoing wars and significant investment, there is not a single high-profile cyber-operation to point to as a success story. The USAF has always been concerned about its continued funding as an independent service. Its existence has been called into question before.<sup>7</sup> At some point the questions will start coming about what it actually means to fly, fight and win in cyberspace. Some air force leaders are thus becoming

concerned about overpromising on cyber.<sup>8</sup>

The confusion is not limited to airmen. The primary role of each military service is to supply war-fighters to the combatant commands. This is understood internally as organising, training and equipping personnel – ‘OT&E’ in the jargon. However, in cyber-security, the services fall short due to their own structures and their failure to internalise training. Despite its problems, the air force is leading the way amongst the services in how it develops cyber-personnel. Even this development is far from adequate: the time spent by a USAF cyber-operator in formal training before conducting highly technical offensive or defensive missions on-keyboard is just nine months. That is nine months from learning what a network is to attacking one. A pilot, by contrast, would receive at least two years’ training in order to reach operational status – and the training will be given by fellow pilots. In contrast, cyber-schoolhouses are understaffed and only around 10 per cent of the military instructors have ever participated in actual cyber-operations.

### *What does it mean to fly, fight and win in cyberspace?*

Cyber-operators, enlisted and officer alike, are expected to be technical experts in all defensive, intelligence and offensive operations despite receiving the same training; the armed forces assume that cyberspace is a single skill to be learned, instead of a domain requiring a variety of unique skill sets. On this, the director of operations for US Cyber Command, Major General Brett T Williams, minces no words: ‘If we are going to treat operations in cyberspace like operations in the other domains, the Services must commit to unique career fields for cyberspace.’<sup>9</sup> Williams also asserts the need for highly technical and experienced operators. Stressing the integrated nature of these operators’ work, he dismisses the idea of isolated cyber-war. As he told the Armed Forces Communications and Electronics Association in February last year: ‘There

is no such thing as cyber conflict ... There’s only conflict.’<sup>10</sup> The director of operations at US Cyber Command should not have to tactfully call out hype while asking the armed services to do their job. It is a small sign of a larger problem.

Cyber-operations offer unique possibilities and opportunities. There have indeed been successful offensive operations that have saved people’s lives, yet the success stories remain classified and so closely held internally that many cannot be shared in training as lessons learned. While classifying sources and methods can protect capabilities, many in the military, the intelligence community, and even in the White House agree that information related to cyber is over-classified.<sup>11</sup> Prompted by the Snowden leaks in 2013, legislators and the public are starting to ask tough questions about actual results and objectives.<sup>12</sup> If successful operations cannot be used to justify investments and improve capabilities and training, they are not really success stories. Hype has caused the military to fall short of its potential. Key to the effective functioning of military services is OT&E – organisation, training and equipment; but the primary output has been ‘HC&C’ – hype, confusion and contracts.

### **Four: Hype Erodes Talent**

Money can attract skill – but it can also push out skill. As organisations spend more and hire more people for their teams, they risk marginalising talent. Experienced team members spend more time on new, untrained members and less time on mission. This is especially evident in the time required to explain technology to inexperienced leaders. The larger the skills differential, the greater the frustration. As more people fill an organisation, the voices of experienced team members also get drowned out and the mission degrades. This problem is acute in government.

The US intelligence community has a rich history of recruiting superb operators and analysts to perform unique and rewarding national-security missions. However, the more recent need for more highly skilled people, especially those with technical training relevant to cyber-security, now risks – perhaps paradoxically – pushing talent out. Each government

team has a set number of people assigned to it, referred to as ‘billets’. When budgets need to be cut, the first thing on the chopping block will be vacant billet slots, sitting idle but nominally costing money. This allows the government to appear to cut costs without causing damage by firing staff or slashing actual budgets. The effect is unfortunate. As a hypothetical example, a team could have up to fifteen vacancies but might have found only eight appropriately skilled people; this team would risk losing the unfilled seven billets. Good leaders will want to help their staff and assigning them to some hot cyber-mission is seen as a sure-fire career booster. So a significant number of people without the appropriate skill sets are assigned to those billets for seemingly good reasons: because it benefits their careers and because it reduces the chance the team will lose that billet. The individual and the team both benefit – but only initially. Once a team comes under pressure to expand the mission and therefore needs staff with the right skills, the slots are already filled. Creating new vacancies is difficult and the hiring process is not geared to the selection of passionate geeks with odd employment records: because of the hype, a large number of career-minded candidates with stellar formal credentials are outcompeting those with nerd credentials and actual experience. Hype drowns talent in a sea of careerists.

### *Cyber-hype makes learning lessons harder*

### **Five: Hype Creates Friction**

Reduced skill means reduced impact and greater friction within organisations. Good cyber-teams will work around knowledge gaps: personnel without the proper skills to complete their mission are usually put into one of two groups. Personnel that are in no way qualified for the mission may fill some sort of front-office or staff position. The other group consists of those that may not have advanced skills, but show some level of aptitude. Both groups, however, consume the time of those capable of performing the mission.



The first group busily orchestrates numerous meetings and presentations and does questionable staff work – constantly requiring clarification from the skilled personnel. It is unfortunately common to have multiple pre-briefings involving numerous personnel prior to a briefing presented to leadership. Meanwhile, the second group often requires extensive on-the-job training, thus turning skilled operators into teachers. The newbies may be eager, professional and willing to learn, but the drain remains, nevertheless. Talented personnel are distracted from the mission. The result is a culture where the best operators consider leaving because of low mission satisfaction and few opportunities for personal growth.

Such friction is not limited to teams. The poorly defined and flamboyant approach to presenting on cyber-attacks makes learning lessons harder. In the military, the time for lessons learned is usually post-operation and post-combat. However, cyber-hype means there is no ‘post-combat’ phase: permanent urgency makes it harder to take a sober and critical look back and to learn from mistakes, thus leading to permanent friction. Operators will be reminded of Clausewitz’s timeless words, which remain applicable even to twenty-first-century cyber-operations: everything is simple, but the simplest thing is difficult.

### Six: Hype Breeds Cynicism

A lack of mission satisfaction means personnel lose connection to an organisation. The outcome is cynicism. Cynicism in the military is often hidden from public view; but this sentiment now reveals itself in military publications and social media. A prime cyber-related example is ‘The Cyber Song’ by a ‘jaded’ USAF major about his experiences in the Pentagon. The song’s theme is confusion, a lack of vision, and bureaucracy. Here is a typical stanza:<sup>13</sup>

So what exactly is this cyber thing, well  
no one knows  
They talk about it all the time though  
mainly just for show  
But once you wear that cyber stink, it  
never goes away  
Your cyber badge and ulcers I’m afraid  
are here to stay

‘Cause it’s cyber-this and cyber-that and  
cyber-ain’t-it-nice,  
But what’s below the cutline when it’s  
time to pay the price  
It’s time to pay the price me-boys, it’s  
time to pay the price.

The DoD’s investment strategy leaves a bitter aftertaste for its own operators: money seems to be available in abundance for contracts, but money is tight when it comes to career and skill development. Managers are focused on budgets and billets, and so they require metrics. The consequence is an emphasis on quantity over quality. It does not matter if you are actually producing anything for the mission, as long as you can give the impression to management that you are doing so. However, showing output and actually creating it are not the same thing. The measure of success, especially for anything cyber-security-related, is usually internal reports, almost always delivered as mind-numbing PowerPoint slide decks that are, according to the jaded major’s lyrics, ‘staffed to hell and back’.

Veritable geeks are passionate about their work, often working late into the night, whether in the office or at home. Such engagement is only sustainable through passion – and sometimes a dash of obsession. When those performing their jobs, within or outside of the government, feel that their talents are being wasted, that they are not being listened to appropriately, or that the mission itself is degrading at the hands of others, there are bound to be strong emotions. Frustration leads to anger. Anger leads to cynicism. Cynicism leads to failure.

### Seven: Hype Degrades Quality

Cynical and overstated reports ultimately lower the quality of bureaucratic procedures and decision-making. First, such reports inform decisions at both the strategic and tactical level. Intelligence reports take highly technical data, combine the information with the interpretations of analysts, and give a bottom line to fill knowledge gaps in the government and guide action.<sup>14</sup> Writing reports on computer-network security requires both technical expertise and

a broad understanding of the field – a combination that is not easily found. Simply put: many of these reports are incomplete or inaccurate.

This, secondly, presents the skilled team members with an unpleasant choice between mission and metrics. Management wants metrics. Thus the team that boasts a 100 per cent increase in the reporting of Chinese intrusions will reap scarce benefits – but that increase could be the result of analysts failing to scrutinise the details. If something is found, the next step is to report it, rather than to validate the information or fix it. (It will take too long and the metric for that instance is still only one.) In some ways, it is the equivalent of the Viet Cong body count in cyberspace: more is better. The result is a twisted incentive structure: prioritising the needs of the mission risks promotion opportunities, award packages and possibly continuation of the mission itself.

### *There is an emphasis on quantity over quality*

Ironically, the Snowden leaks have brought some of this problem into the open: in the bureaucratic setup of a large intelligence agency, presentation skills can become more valuable than coding skills. It gets worse once it dawns on ‘PowerPoint warriors’ that technical jargon works like magic on superiors who may not fully grasp the details.<sup>15</sup> The US intelligence community is coming to terms with this now, as some of its programmes have come under increased scrutiny from law-makers and the public. However, most journalists writing about the leaked material do not understand the limitations of these documents. Some of the revealed slide decks are put together by non-technical team members, or by staff who deliberately misrepresent the mission and overstate capabilities for internal, bureaucratic reasons: to get more internal funding for their project and their team, to get the business trip abroad or simply to get promoted. Hype means that upper echelons in government should carefully

check the quality of internal documents. Hype also means that the public cannot take everything that is leaked as fact. Spoiler alert for Snowden slide addicts: your favourite PRISM deck may be stacked to 'sex it up' for good effect in the office.

### **Eight: Hype Weakens Products**

In the private sector, hype means that the buzz generated can be worth more than products. In cyber-security, the market is duped too easily. Most users readily accept that a piece of software on their machine that should block malware and intruders does not actually block every exploit out there. It is, unfortunately, a common view that the hacker will always get through, to paraphrase Stanley Baldwin.<sup>16</sup> The bar hangs low: consumers do not expect bulletproof cyber-security products and services. Firms get away with doing a reasonably good job and market pressure remains lower than it should be.

Paradoxically, this is a result of hyped-up threats. The consequence: a company's market value is driven up not by products that actually work, but by standing out in the news cycle and creating buzz. Often this is done through bold claims, grand ideas for future products, and fancy reports.

### *Most journalists writing about leaked documents do not understand their limitations*

Industry buzz attracts top cyber-security talent to fill jobs, convinces consumers to purchase products or services, and opens up the option of being acquired by a larger company – which attempt to win large contracts and fill strategic markets by acquiring smaller companies with products or services they do not currently possess. Perception is key in such instances. These buyouts target cyber-security companies that have been around for a relatively long period of time, such as Cisco's \$2.7-billion acquisition of

Sourcefire;<sup>17</sup> companies that are of medium relative age, such as FireEye's \$1-billion acquisition of Mandiant;<sup>18</sup> or brand new companies, such as Palo Alto Network's \$200-million acquisition of Cyvera.<sup>19</sup> The most coveted cyber-security companies specialise in incident response and malware protection. The large sums of cash involved create a culture where new cyber-security companies risk being more focused on grabbing attention for buyouts than on producing high-quality products.

The hype around cyber seemingly benefits the companies acquiring the smaller companies as well. Following the announcement of FireEye's acquisition of Mandiant, for example, the former's stock rose by over 38 per cent. A senior investment partner at a major venture-capital firm who invests in cyber-security companies pointed out that when considering an acquisition, many of the larger companies are not primarily concerned with the quality of the product or service of the smaller company. Instead, they care about the target area and the headlines that the companies are getting. The larger company stands to profit more through the rise of its share value than from the acquired products themselves. Shareholders and investors get excited, freeing up more capital.<sup>20</sup> The result is an all-too-familiar dynamic that values excitement about ideas for future products more than actual solutions in the here and now. However, caution is in order: if there is a cyber-bubble, it can go 'ping'.

### **Nine: Hype Clouds Analysis**

Cyber-espionage does take place, and on a major scale; but facts and digital forensics do not speak for themselves and hype weakens the analysis. Over the past few years, vast and systematic secret campaigns to steal trade secrets and intellectual property have been brought into the open. Security companies such as Kaspersky Lab, Symantec, McAfee, Mandiant, CrowdStrike and others have created a vibrant market of reports, usually with funny names emulating secret codenames. These reports portray espionage incidents in sometimes impressive detail. Recent examples are Kaspersky Lab's 'Unveiling "Careto"' report,<sup>21</sup> published in February, or

Symantec's 'Dragonfly' report, published in June.<sup>22</sup> The quality of these reports varies, but often these companies treat them more as marketing opportunities, hinting at potential perpetrators based on speculation extracted from the campaign's setup and the malware itself. In several of these reports (for instance, in 'Unveiling "Careto"'), the highlighted attributive evidence is language settings – which in the case of Spanish is a rather imprecise indicator. Of course, some company reports on Advanced Persistent Threats are better than others. Nonetheless, increased competition in 'Advanced Persistent Marketing', as an industry joke has it, runs the risk of driving down the quality of analysis of these reports. Nevertheless, in a climate of general hype that also lacks technical insight, even mainstream news outlets very rarely call out poor quality.

### *A climate of general hype lacks technical insight*

The indictment by the US Department of Justice in May 2014 of five serving members of the most prominent Chinese espionage unit, PLA Unit 61398, added yet more detailed evidence to the influential 'APT1' report on the same unit, published by Mandiant about a year earlier.<sup>23</sup> However, the indictment left many questions unanswered. Nevertheless, US authorities were over-eager in hot pursuit. Wild West-style 'Wanted by the FBI' posters were splattered across the international press, designed in bright red, complete with mug shots of the five Chinese 'thieves'. Instead of such overt provocation, the US government could have included a more realistic interpretation of Chinese activities, if not in the indictment then certainly in the political statements that came with it. The Department of Justice could have pointed out what a solid and hype-repellent intelligence analysis would surely bring to light – that what looks like state-controlled Chinese cyber-espionage from the vantage point of the Western District of Pennsylvania looks rather different from Beijing: it looks like a lack

of state control and deeply entrenched corruption. It is highly likely that various PLA units receive some of their tasking not only from their civilian leaders in the Communist Party, but also through shady backchannels and personal connections directly from state-owned enterprises that are taking advantage of idle PLA resources. The kind of targeting and tasking that the indictment revealed is probably too precise to be requested by senior government officials. Pointing this out would have been more embarrassing for Beijing – as well as being more difficult for it to counter – and diplomatically less damaging. Lower the pitch, and 61398 is code for China's weakness rather than its strength.

### Ten: Hype Kills Nuance

The debate about cyber-security in political science and international relations has been very visible among policy elites. Policy-makers and their advisers read *Foreign Affairs* and *Foreign Policy*. However, political and social scientists often do not appreciate the technical details of network breaches, or security setups in critical infrastructure and industrial plants. Public-policy experts too often treat computer scientists and engineers as token experts. It is not uncommon in Washington or London to invite one or two technologists to a roundtable on cyber-security at a foreign-policy think tank or international-relations workshop at a university. These experts are then expected to field questions ranging from cryptography to network exploitation, to vulnerability markets to industrial control systems; but such universal technology experts do not exist. The equivalent would be expecting political scientists trained in Afghan cultural history to explain the dynamics of the German political-party system.

Most political scientists also lack the technical skills to call out poor-quality company reports or government documents. Instead, too many scholars seem happy to engage in self-referential theoretical debates of little relevance to anybody else – for instance, on the 'securitisation' of cyber-security. On the other end of the spectrum, many a computer scientist considers security as 'too low down in the stack' to be

interesting academically,<sup>24</sup> although more funding may help to focus the mind. Furthermore, most prefer technical solutions, neglecting the required fingertip-feel for the intricacies of political decision-making. Hype keeps debates isolated and pitched at such a high level of abstraction that attention to crucial details seems permanently in short supply. As a result, the quality of the broader debate remains as frustratingly low as the 'ivory tower' remains high.

### Eleven: Hype Escalates Conflict

Government, military and industry leaders are consequently able to make wild claims without providing evidence. This has an escalatory effect. 'We're in a pre-9/11 moment, in some respects, with cyber,' said John Carlin, assistant attorney general for national security in the Justice Department in Aspen, Colorado in July.<sup>25</sup> He did not provide concrete details to back up his claim. Just weeks after Russia annexed Crimea in March 2014, NATO's Supreme Allied Commander Europe (SACEUR), USAF General Philip Breedlove, made comments about Russia's use of cyber in doing so. He told the *New York Times* that cyber-warfare had been used to isolate the Ukrainian military on the Crimean peninsula.<sup>26</sup> A month later he revisited these claims, stating that cyber was a critical part of Russia's actions. To quote Breedlove:<sup>27</sup>

When they [Russia] took Crimea, cyber was a part of a well-planned, total decapitation of Crimea from the command and control structure of Ukraine. Ukraine was absolutely disconnected from being able to do anything with their forces in that area. Cyber was one of three tools used, and used quite exquisitely.

Consequently, the Atlantic Alliance is updating its cyber-defence policy – a point confirmed at the recent NATO summit in Wales. A very serious cyber-attack, some in the Atlantic Alliance seem to suggest, should be treated like an invasion. 'For the first time we state explicitly that the cyber-realm is covered by Article 5 of the Washington Treaty, the collective defence clause,' said Jamie Shea, NATO's deputy assistant secretary

general for emerging security challenges, in June.<sup>28</sup> At first glance, this statement appears to be meant as a deterrent.

However, deterrence does not seem to apply: to deter, a statement needs to be clear and backed by credible threat of punishment. So far, NATO is doing the reverse: 'We do not say in exactly which circumstances or what the threshold of the attack has to be to trigger a collective NATO response,' Shea said, 'and we do not say what that collective NATO response should be.'<sup>29</sup> A vague but high bar for cyber-attacks also implicitly legitimises ongoing espionage attacks as acceptable and minor. Moreover, the vast majority of cyber-attacks also do not fall into NATO's remit in the first place: espionage and cyber-crime are problems for intelligence agencies and law enforcement, not for a military alliance. For militants and the Kremlin, the subtext is clear: cyber matters; better up your game. NATO – among others – is escalating a problem that *someone else* will have to solve.

### Twelve: Hype Feeds Hypocrisy

When confronted with these arguments, NATO officials concede that the real reason for the new posture was not operational, but deeply political: NATO wants to put pressure on smaller countries to spend more money on their cyber-defence capabilities, various Alliance officials recently confirmed to the authors during a visit to NATO's Brussels headquarters.<sup>30</sup> Updating the Alliance's cyber-defence clause, these officials believe, would help to compel smaller member countries to make much-needed investments in equipment, staff and training.

*NATO is escalating a problem that someone else will have to solve*

Perhaps this was the reason for General Breedlove's bold claims on Ukraine. For there was no evidence that cyber-attacks played a significant role in 'decapitating' Crimea – certainly not in the public domain. Nor did the general provide any details to back up his statement. If the evidence was contained in classified reports the analysis could be

made public without revealing sources and methods. The situation between Russia and the West is heated. It is therefore ever-more important to keep an intangible debate sober in tone and grounded in fact in order to avoid escalation. If political or military leaders make statements about, for instance, a commercial airliner thought to have been downed by Ukrainian rebels, journalists and the public more broadly would expect at least some evidence to back up such statements of attribution. Not so in 'cyber': expected standards of proof are missing.

## *Hype damages the public's trust and confidence in the Internet*

It is almost 2015: cyber-security is not a novel problem any more. Companies as well as political leaders should not get away with bold yet unsubstantiated statements made for good effect.

### **Thirteen: Hype Undermines Trust**

Hype damages the public's trust and confidence in the Internet and, ultimately, in their own governments. Inter-state conflict makes the public uneasy. Tension between states has a real social and economic impact. It is easy to see Russian troops invading Crimea on television and it would also be possible to see Russian troops withdrawing from Crimea. This visually defined 'beginning' and 'end' to events lessens tension and public concern. However, there is no visible beginning or end to cyber-conflict. Instead, the public relies on what it hears from governments, journalists, academia and industry; and their message is loud and clear: the grid could be hacked at any time, the lights could go out, financial markets could collapse, bank accounts could be raided, competitiveness could be lost to China. Some of these scenarios are certainly possible; but this constant barrage is sowing fear, uncertainty and doubt – 'FUD', in the jargon. When the predicted calamity seemingly does not happen, doubters instead start to

wonder if the FUD could perhaps be a smokescreen for something else.

The DoD likes to remind the public again and again that cyberspace is a new battlefield, a 'new domain of warfighting'. The leaks drip-fed by the NSA and the UK's GCHQ (Government Communications Headquarters) during the course of the last year have consequently left a bitter aftertaste for many; and the outrage increases from the political centre towards the fringes, with one argument suggesting that on this new, high-tech battlefield, governments are fighting against their own citizens. This is a deeply misguided view. The divisions in this highly emotional debate are deepening, even if the self-described anti-surveillance activists are not getting as much resonance as they had expected. The US and UK governments and intelligence agencies actually have a convincing response: do not speculate, they say – your evidence is not good, pay attention to details and do not overstate the problem. However, the governments' propensity to do the same thing themselves with regard to cyber-security – to speculate, generate hype and ignore the finer detail – has led rightfully frustrated citizens to lose trust in their elected officials. This careless attitude towards public support is now biting back.

## *The intelligence community should see the Snowden leaks as an opportunity*

This contradiction is made worse by the nature of digital forensic evidence. In diplomatic or military confrontations, evidence becomes increasingly available and clearer as time passes; history clarifies itself as archives are opened, documents are declassified, participants write memoirs and give interviews, eyewitnesses come forward and photographs emerge. In the case of cyber-confrontations, however, evidence degrades over time: forensic artefacts are more ephemeral to begin with, being literally scattered across the globe. Lines of arcane code are not

nearly as convincing as the discarded casing of a large projectile or a picture of a missile launcher. Worse, log files will be deleted, computers replaced and physical connections changed. This makes any conflict in cyberspace highly prone to doubt and conspiracy theory. It takes more effort and evidence to disprove alarmism and hype in cyberspace than it does to generate it.

### **Now What?**

The 1983 film *War Games* (a Cold War science-fiction classic) is about a colossal computer – known as Joshua – which controls America's nuclear arsenal and is tricked by an unsuspecting teenage hacker into playing war. By the end of the movie, the supercomputer is ready to launch an all-out nuclear attack against the Soviets. Joshua was based on NORAD's SAGE (Semi-Automatic Ground Environment) air-defence system, a technology that in many ways enabled modern computers and the Internet. As the machine cycles through all of the potential war scenarios, it finds that they all result in calamity and defeat. 'The only winning move is not to play,' Joshua concludes.

Today the hype machine has full momentum; it practically controls the debate – and it is self-defeating. In a democracy, government, the press, academia and industry are supposed to keep each other in check, to balance each other. Political opposition, editorial fact-checking, scholarly peer review and business competition should calibrate output and lead to progress over time. Old-fashioned cyberneticists and control engineers call this *negative feedback*. It is what creates stable systems and balance, keeping machines humming steadily instead of pushing them into overdrive. Cyber-hype has created a culture without checks and balance – it is *positive feedback*, in engineering lingo, pushing systems to overheat or overpressure, and finally to crash. Put simply, the hype is not sustainable, raising the question of what should be done.

Senior officials should know their tech – or at least the basics; indeed, a cyber-security leader needs sufficient technical knowledge to cut through the hype and see the real challenges and



limitations. In the military, generals and flag officers should value personnel with hands-on expertise over career staff officers, especially when making decisions about awarding large contracts. The intelligence community should see the Snowden leaks as an opportunity and continue to open up: the community's attributive capabilities now have increased credibility even if few details are disclosed, the public now has a slightly better grasp of its work, and better explaining possibilities and especially limitations can strengthen democratic institutions. Industry leaders should expect that the 'cyber-gold rush' will subside at some point, as the gap between their clients' overblown fears and real losses slowly shrink; caution is thus in order because hype can echo back as reputational damage. Editors should keep journalists with specialist knowledge focused on the technology beat, check their facts, and ask hard

questions of officials and industry techies; they should not let generalists get away with copy-pasting press releases – and for this, watchdogs are needed, not hand-reared puppies. Scholars of all stripes should do what sounds easy but is actually difficult: first, get the facts right, and then make a more concerted effort to look beyond their narrow disciplinary horizons and speak plain English. Privacy activists, finally, should halt their own cyber-hype and stop pretending that the NSA and GCHQ have limitless surveillance and espionage capabilities. The general public deserves a better debate on cyber-security.

The bubble, no doubt, will eventually pop. After all, defence is doable, results matter, and attention to detail is crucial. Change is influenced from the top but it is aided by every person who chooses to forgo hyperbole. So, take advice from the machine, listen to Joshua, and do not play the game of cyber-hype. ■

*Robert M Lee is an active-duty USAF Cyber Warfare Operations Officer who has led multiple cyberspace operations programmes in the Air Force and US Intelligence Community.*  
Twitter: @RobertMLee

*Thomas Rid is a professor in the Department of War Studies at King's College London. He is author of Cyber War Will Not Take Place (Oxford University Press/Hurst, 2013) and is currently working on a book about the history of cyber-security.*  
Twitter: @RidT

*The authors would like to thank Ben Buchanan.*

*The opinions and statements expressed by the authors are their own and do not represent or constitute an opinion of the United States Government, Department of Defense, or US Air Force.*

## Notes

- 1 Amir Mizroch, 'Top U.K. Cyber Cop: Russian Hackers Are Our Biggest Threat', *Wall Street Journal*, 30 June 2014.
- 2 Martin Giles, 'Defending the Digital Frontier', *The Economist*, Cyber-Security Special Report, 12 July 2014.
- 3 Nick Simeone, 'Hagel Outlines Budget Reducing Troop Strength, Force Structure', DoD News, 24 February 2014, <<http://www.defense.gov/news/newsarticle.aspx?id=121703>>, accessed 18 September 2014.
- 4 Amber Corrin, 'Defense Budget Routes At Least \$5B to Cyber', *Defense News*, 4 March 2014.
- 5 MuckRock, 'FOI Request: Booze Allen Hamilton Contracts (Air Force)', 14 March 2013, <<https://www.muckrock.com/foi/united-states-of-america-10/booze-allen-hamilton-contracts-3368/#628658-contracts>>, accessed 18 September 2014.
- 6 Lockheed Martin, 'Lockheed Martin to Assist Department of Defense in Fight Against Growing Threat: Cyber Crime', press release, 3 May 2012, <<http://www.lockheedmartin.co.uk/us/news/press-releases/2012/may/isgs-DC3-EITS-0503.html>>, accessed 18 September 2014.
- 7 Robert M Farley, *Grounded: The Case for Abolishing the United States Air Force* (Lexington, KY: University Press of Kentucky, March 2014); Jeff Schogol, 'Columnist Argues for Abolishing Air Force', *AirForceTimes.com*, 12 January 2014.
- 8 Author conversations with various senior officers in the US and UK air forces over the past months.
- 9 Brett T Williams, 'The Joint Force Commander's Guide to Cyberspace Operations', *Joint Forces Quarterly* (Vol. 73, No. 2, April 2014).
- 10 C-Span.org, 'U.S. Cyber Command Operations', speech given by Major General Brett T Williams, operations director at US Cyber Command, to Armed Forces Communications and Electronics Association, 22 February 2013, <<http://www.c-span.org/video/?311129-1/us-cyber-command-operations>>, accessed 18 September 2014.
- 11 Authors' personal conversations with various cyber-security officials, August and September 2014.
- 12 See, for instance, Privacy and Civil Liberties Oversight Board, 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', Washington, DC, 23 January 2014, <<http://www.pclob.gov/meetings-and-events/2014meetingsevents/23-january-2014-public-meeting>>, accessed 22 September 2014.
- 13 Jadedmajor, 'Cyber Song', YouTube, 8 January 2014, <<http://www.youtube.com/watch?v=MpMBETNC-44&feature=youtu.be>>, accessed 18 September 2014.
- 14 US Department of Defense (DoD), 'Joint Publication 2-0: Joint Intelligence', 22 October 2013, <[http://www.dtic.mil/doctrine/new\\_pubs/jp2\\_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf)>, accessed 18 September 2014.

- 15 Several of the files leaked by Edward Snowden provide examples of overstated or misrepresented capabilities. One TOR-related slide deck, codenamed 'EgotisticalGiraffe', offers an especially lucid example. See <<http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document>>, accessed 22 September 2014.
- 16 'The bomber will always get through', Stanley Baldwin famously said in a speech to Parliament in 1932. See Keith Middlemas and John Barnes, *Baldwin: A Biography* (London: Weidenfeld and Nicolson, 1969), p. 735.
- 17 Cisco, 'Cisco Completes Acquisition of Sourcefire', San Jose, California, 7 October 2013, <<http://newsroom.cisco.com/release/1273122>>, accessed 22 September 2014.
- 18 Jim Finkle, 'FireEye Buys Cyber Forensics Firm Mandiant For About \$1 Billion', *Reuters*, 2 January 2014.
- 19 Palo Alto Networks, 'Palo Alto Networks Completes Acquisition of Cyvera', Santa Clara, California, 10 April 2014.
- 20 Robert M Lee's discussions with a senior partner of a Fortune 50 venture-capital firm, US, 8 April 2014.
- 21 Kaspersky Lab, 'Unveiling "Careto": The Masked ATP', 11 February 2014, <[http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask\\_v1.0.pdf](http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf)>, accessed 18 September 2014.
- 22 Symantec, 'Dragonfly: Cyberespionage Attacks Against Energy Suppliers', Version 1.1, 30 June 2014. For the latest version of the report, see <[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/Dragonfly\\_Threat\\_Against\\_Western\\_Energy\\_Suppliers.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf)>, accessed 18 September 2014.
- 23 Mandiant, 'APT1: Exposing One of China's Cyber Espionage Unit', 18 February 2013, <[http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)>, accessed 18 September 2014.
- 24 'Too low down in the stack' is lingo for questions that are concerned with the lower layers of the widely used OSI model.
- 25 Bill Gertz, 'Al Qaeda Targeting U.S. Infrastructure for Digital 9/11', *Washington Free Beacon*, 24 July 2014, <<http://freebeacon.com/national-security/al-qaeda-targeting-u-s-infrastructure-for-digital-911/>>, accessed 18 September 2014.
- 26 Michael R Gordon, 'NATO Commander Says He Sees Potent Threat from Russia', *New York Times*, 2 April 2014.
- 27 As quoted by Murray Brewster, 'NATO Scrambles to Stitch Together a Cyberwar Strategy in Face of Attacks', *Canadian Press*, 6 May 2014.
- 28 Steve Ranger, 'NATO Updates Cyber Defence Policy as Digital Attacks Become a Standard Part of Conflict', ZDNet, 30 June 2014, <<http://www.zdnet.com/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict-7000031064/>>, accessed 18 September 2014.
- 29 *Ibid.*
- 30 Personal author communications at NATO, Brussels, 8 July 2014.

## Submissions

The Editor invites the submission of unpublished manuscripts on all topics related to international and national defence and security issues, and military history.

All contributions to the *RUSI Journal* are subject to peer review by the editorial board.

Guidelines for submissions can be found at the back of the *Journal* or at [www.rusi.org/submissions](http://www.rusi.org/submissions)

## Letters to the Editor

The Editor welcomes correspondence from readers on articles or reviews, and other matters arising from discussions in the *RUSI Journal*.

Please mark all letters for the attention of the Editor, and send to [publications@rusi.org](mailto:publications@rusi.org) or to Dr Emma De Angelis, RUSI, Whitehall, London SW1A 2ET, United Kingdom.

Publication in the *Journal* is at the discretion of the Editor. Anonymous letters will not be considered.