Cyber-physical attacks:
Dawn of a new age in cyber-warfare?

Authors
Christopher Cope, MSc (Royal Holloway, 2016)
John Austen, ISG, Royal Holloway

Abstract

Cyber attacks are frequently in the news, including the new phenomenon of cyber warfare. But how worried should we be? Whilst other investigations of this topic look at the means of attack, this paper explores the impact. Can cyber attacks really have a significant impact? This paper will be of interest to anyone who has an interest in the application of cyber power in international relations.[a]

[a]This article is published online by Computer Weekly as part of the 2017 Royal Holloway information security thesis series `http://www.computerweekly.com/ehandbook/Cyber-physical-attacks-Dawn-of-a-new-age-in-cyber-warfare`. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full MSc thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/isg/research/technicalreports/technicalreports.aspx`.

In the control room, engineers nervously watch their screens. Can this really be happening? Before their eyes, some malevolent force is controlling their computer and, one by one, vital components within their network were shut down, condemning thousands of locals to a night of misery without power, in freezing temperatures. If this sounds like a scene from a Hollywood blockbuster, it is in fact real life. These events occurred on 23rd December 2015 at the Prykarpattyaoblenergo power distribution control centre in western Ukraine following a cyber-attack.

The ability to hack and remotely control a remote computer is not new, but cyber-attacks influencing physical space is a more recent phenomenon and one which is capturing the headlines. Cyber-attacks against computer systems which only compromised information have been a known downside of an increasingly interconnected world for some time, but beyond private data entering the public space or the loss of a website for a period of time, what was the actual impact from a national perspective? Individual companies may suffer through cyber-crime, but such incidents are not going to fundamentally change government policy. Are cyber *physical* attacks somehow different? Can an impact, initiated by a cyber-weapon, that is manifested in the physical domain be sufficiently serious to be comparable to that which could be inflicted by more traditional means of warfare, for example the destruction caused by high explosive? In what has become a polemic debate, opinion is divided between advocates of a revolutionary new method of warfare, and those who believe it to be an out of control marketing campaign.

Cyber Physical Attack

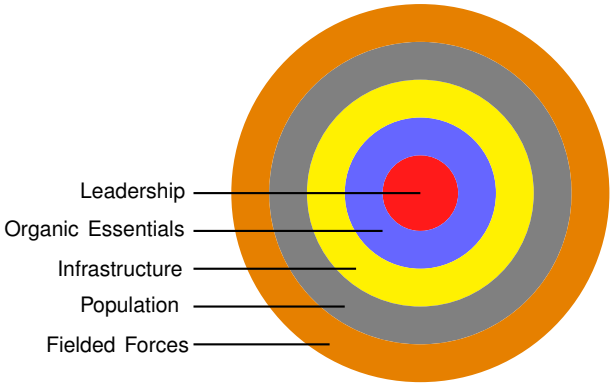
A particular category of cyber attack that, deliberately or accidentally, adversely affect the physical domain by affecting the control and communication infrastructure which connect devices, sensors, actuators and other mechanisms with their operators.

In examining the potential of cyber warfare, a number of academic and practical questions present themselves. How does cyber-warfare fit into our understanding of conflict, and is it time to review Clauswitzian theories of conflict (emphasising physical violence and the primacy of the state in conflict) which date back to the 18th century? What impact could a cyber-attack have against an advanced military platform, or for that matter against a military force with very low reliance on technology? And can a cyber-attack bring a nation to its knees? For the purpose of brevity, this paper will focus on the last question (at least in part). Can cyber physical attacks have an impact at a strategic level? I will also be focusing only on the use of aggressive cyber activity in support of political objectives, not those of a criminal nature for financial gain, although the line is occasionally

blurred.

The strategic environment

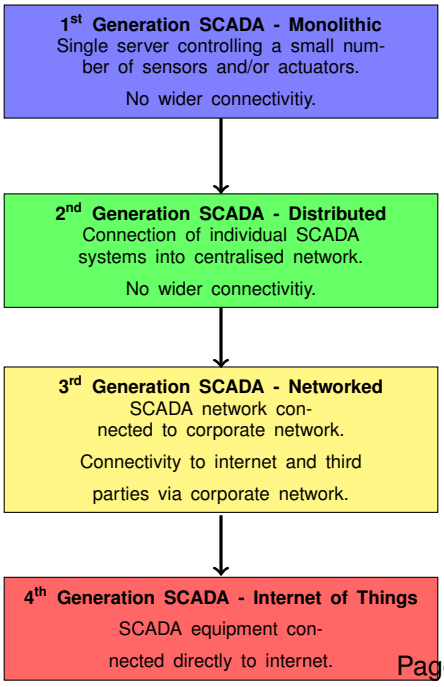
In using the term “strategic level” I am referring not to a country’s military, but instead those aspects of a nation state that may support or direct that military, the “inner rings” on the diagram below. These include infrastructure, the general population, political leadership and organic essentials (which could include the emergency services, financial institutions and other key organisations which are essential to the continued operation of that society). Cyber-attacks can by-pass the battlefield and strike at the heart of an opponent; and the greater the reliance on cyber-space the greater the potential impact. The key question is how significant those impacts could be.



Attacks at the strategic level can focus on three areas. Firstly, the ability to influence the population of a potential opponent, or neutral, country through internet dissimulated propaganda. When one looks at recent confrontations, such as Ukraine and Georgia, the physical actions on the ground are accompanied by a blizzard of propaganda designed to undermine the enthusiasm of third parties to intervene. Potentially, such propaganda could also influence opinions during other key events; for instance the US presidential campaign as recently alleged. Another potential method would be to attack critical strategic IT systems purely within the cyber-domain. Financial institutions are heavily reliant on systems such as SWIFT; an attack here could cost huge amounts of money, maybe even enough to influence national policy. However, this paper will focus on the third area and the newest phenomenon in cyber-warfare: the cyber physical attack, the form of warfare which is perhaps the most recognisable to devotees of traditional warfare.

Cyber-physical attacks

In the Aurora Generator Test, researchers from the Idaho National Laboratory used a computer programme to rapidly open and close a generator’s circuit breakers out of normal sequence, eventually causing it to explode. Other examples have proven that it is possible to influence cyber-physical systems in the real world.



Hackers have managed to obtain access to so called SCADA systems on a number of occasions. Supervisory, Control and Data Acquisition (SCADA) is a term used to cover a wide range of operational technology, but they basically support in the monitoring or direct control of machinery or other equipment. From basic origins, they have evolved over time, with greater interconnectivity (and risk) as they developed.

This wider connectivity has exposed many of the inherent vulnerabilities in SCADA networks previously masked by their standalone status. MODBUS, for example, is an old communication protocol that is still used today and where

poor authentication allows spoofing. The DNP3 architecture (a set of communications protocol used in process automation systems) lacks encryption and also has issues with authentication. Whilst software companies are making efforts to improve the security of such networks, they may in many cases lack the robustness that one would expect in a modern corporate network. Given the sporadic nature of the drive to connect these systems, many may be connected in ways which administrators are unaware of. It may also be difficult to update elements of a system which is operating an array of operating systems and applications which have required considerable effort to configure, and on which updates may have an unknown effect. All of this of course assumes that the organisation places sufficient importance on cyber and information security. Sky News reported that over half of the NHS Trusts they surveyed in November 2016 could not identify how much they were spending on cyber security, whilst others spent nothing. Without backing by senior leadership and appropriate resources, cyber-security is doomed to fail.

In 2011, a hacker called pr0f managed to obtain access to a Siemens produced SCADA network controlling a water treatment facility in Houston, Texas. The attack was successfully executed in less than 10 minutes, exploiting a weak 3 digit passcode. In that instance, the attacker merely wanted to highlight a vulnerability, but what if the motives were less benign? Stuxnet was the first high profile cyber physical attack and provided evidence that the physical domain could be influenced via cyber-space. Whilst a debate rages over the impact Stuxnet had on Iranian uranium production (ranging from negligible to a delay of 5 years), the important fact is that such an attack has been proven to be possible, and arguably the psychological effect on the Iranian leadership facilitated diplomatic negotiations, whilst preventing direct action by the Israelis.

Stuxnet

Deployed in an attempt to de-rail Iranian development of nuclear material, the Stuxnet worm targeted the SCADA systems controlling the centrifuges. Estimates vary between 800 and 2000 damaged centrifuges before the worm was discovered.

The development of SCADA systems has not stopped at the 3rd generation; the next generation is being developed and implemented in the Internet of Things. Here the use of technology to monitor and control devices has grown exponentially, ranging from sports wearables to medical equipment. But has the security of these systems kept pace? A number of security reports have highlighted serious concerns, including authentication over networks, confidentiality of data and the ease by which a denial of service attack could be launched. It certainly seems like the drive for operability has come at a cost to security, a situation not dissimilar to the original development of SCADA systems. Clearly, whilst a hack on some IOT devices will be merely annoying, there is potential for critical systems to be targeted, particularly in healthcare, and for that impact to be lethal.

Attack constraints?

Attribution is an acknowledged difficulty with cyber-attacks. Just because a computer in a particular country can be proven to have instigated an attack, it is far more difficult to tie that computer and its users to the policy of that country's government. So why have we not seen more cyber physical attacks, including far more serious examples? A potential constraint is legality. A wide scale attack on civilian infrastructure would almost certainly be a breach of the laws of armed conflict as recognised today. Military actions are bound by military necessity, distinction and proportionality. In other words, attacks must be directed against other combatants and every effort should be taken to limit the impact on non-combatants. There may be occasions when traditional methods would be directed against combatants located within civilian infrastructure (under military necessity principle), but this should be a last resort. How then could a cyber-attack, against a power station serving thousands of non-combatants, be justified? If the aim is to disable or destroy the power generated, then it must be questionable what military aim that is serving? If an enemy combatant is using the power plant as

cover, then it is highly unlikely that a cyber attack against the power plant will have any impact on the military unit itself. Suddenly the use of cyber warfare at the strategic layer is not as clear cut as some suppose it might be.

There are suggestions that a cyber attack just can't inflict enough damage to be taken that seriously. In their book, *Cyber War versus Cyber Realities* (published by Oxford University Press in 2015), Valierano and Maness evaluate a huge range of cyber-attacks (including information hacks for espionage purposes) that dated up to and including 2011. The overwhelming majority of these attacks were very low impact, with only one achieving a mid-level impact rating (Stuxnet). The authors question if the threat of cyber warfare has been inflated; a point that is echoed by author Thomas Rid in his book *Cyber War Will Not Take Place* (published by Hurst and Company in 2013), who points out with some validity that no one has died yet because of a cyber-attack. At first glance their argument is convincing, but perhaps, as I am about to explore, there are good reasons why cyber combatants are pulling their punches, even when they may ignore many aspects of the laws of armed conflict when deploying traditional military force.

In 2011, the US formally declared that they would respond to a cyber-attack with traditional military force, if the situation warranted it. But how serious would a cyber-attack have to be in order to trigger that response? American officials have repeatedly blamed state sponsored hackers in China and Russia for a number of hacks against government and commercial targets, but no military action has been taken. I would suggest that this is because such a retaliation would be viewed as grossly disproportionate to the impact achieved by the hacker and would be very difficult to justify to the general population. The alleged Russian hacks against presidential candidate Hilary Clinton are an obvious affront and potentially breach international law, but the US is also obliged to ensure any response is proportionate. However, consider this scenario. A cyber physical attack disables power plants in a northern US State for a period of days, or even weeks, during winter and people die as a result of hypothermia and other cold related medical conditions. What about if a cyber-attack caused major disruption to the US air traffic control network, or caused a major incident at a nuclear power plant? Would the loss of life (let alone a mass casualty event) be so easily shrugged off by a victim government? Causing loss of life is the red line in international relations that Valierano and Maness refer to, and one which is not lightly crossed in normal circumstances.

Those powers who are capable of launching sophisticated cyber-attacks against each other have not come into direct conflict in recent years, certainly since the dawn of cyber warfare. Would this situation change if a direct conflict existed? In my opinion almost certainly. In a major conflict, strategic targets would be more likely to become a target, particularly if strategic targets in the west were attacked first. The laws of armed conflict may present challenges but how exactly would they be observed in the event of a major conflict? To quote the air-power theorist Douhet, when an enemy's strategic infrastructure looks like a quick route to victory in a costly war, legal niceties will be "swept away like dried leaves on the winds of war".

But if a nation state feel constrained by this political red line, what about a terrorist group? Stuxnet cost $100 million to develop and the resources of a major cyber power, but as any weapon type develops, the entry level requirements fall. Malware is obtainable on the Dark Net and hacking skills can be bought; whilst the sponsoring of a terrorist group by a nation state that wishes to remain anonymous cannot be overruled. Protest actions like mass Distributed Denial Of Service attacks in support of a cause may be more of a motivation for activists, not terrorist, but the ability to cause real physical damage with little risk will surely be a temptation. Not all straight forward malware attacks have been successful however. The Davis-Besse incident in Ohio did not result in major failure and the complexity of operating systems and applications can slow the impact of malware. The Ukrainian incident mentioned in the opening paragraph probably relied on an initial hack or malware insertion to obtain control of the system, followed by exploitation by someone who knew

Davis-Besse nuclear power plant

The nuclear power plant's SCADA systems were infected with the Slammer Worm in 2003, leading to a safety control system being taken offline for 5 hours. The malware was inserted via a contractor's laptop accessing the plant's corporate network remotely.

how to inflict the required amount of disruption. This points to a level of additional knowledge that may not be readily available to a terrorist group, although that does not mean that such knowledge could not be provided.

One must also question whether the loss of cyber-reliant infrastructure would be sufficient to cause a significant change to an opponent's strategy. Creating a critical event in a power plant would of course have a major impact, but civilian populations have proven themselves to be amazingly reliant in the face of aerial bombardment and terrorism - at least when the objectives of the war are widely supported. For example, the conventional aerial bombardments of the Second World War failed to deliver a knockout blow against a population which either supported their country's war aims, or were too cowed to object. Yet, following the Madrid railway bombings prior to the 2004 elections, which were a revenge attack for Spain's involvement in Iraq, the Spanish opposition won an unexpected victory as a result of the anti-war feeling of the electorate, resulting in Spain withdrawing its troops shortly afterwards. If the nation's policy is widely supported then minor inconvenience, or even mass casualties, won't necessarily undermine that support. But the same deprivations will be less well tolerated for a conflict in a foreign land about which the general public know or care little. Would the general public continue to support its government's foreign policy when healthcare devices are remotely disabled, leading to widespread casualties?

A view of the future?

Without doubt, some of the wilder assertions that cyber warfare will replace traditional means are unrealistic. However, cyber-warfare has a real place in modern conflict, as a means to maintain a low level diplomatic hostilities, in support of traditional methods or as a standalone, strategic option against computer-dependent systems. Cyber-physical attacks thus far should serve as a wakeup call and there is no reason why any organisation cannot take appropriate action to protect their own networks. Certainly, those who manufacture or operate 3rd or 4th generation devices and systems that can be classified as critical must ensure that those systems are developed with security in mind, not as an afterthought. We have not yet seen a major cyber-physical attack which has cost lives, but as capabilities develop this will surely occur at some point. When air power first emerged in the early 20th century, it was largely written off by traditionally minded generals and admirals who looked at the flimsy flying machines with incredulity. Yet within 30 years, those early aviators had seen their barely airworthy machines develop into sophisticated weapons which played a decisive part in the land and sea domains, as well as delivering independent strategic effect. This may well be the dawn of the age of cyber-warfare and it would be wise to consider how to defend against potential threats before they are realised.

Biographies

Christopher Cope is an information assurance professional currently employed by the National Nuclear Laboratory. He has previously served in the Royal Air Force Police for 14 years, including tours as an MOD Accreditor, Chief Information Security Officer and Head of Information Assurance to British Forces operating in Afghanistan. Following his departure from the Royal Air Force, he worked as an Information Assurance Consultant, delivering security solutions to a range of public and private sector organisations before taking up his current role. He has recently passed with distinction the MSc Information Security course at Royal Holloway and has interests in information security management, risk and the development of the cyber domain within international relations.

John Austen (BA, MSc, FBCS, NEBSS) is a consultant lecturer in the Information Security Group at Royal Holloway University of London. He is a specialist in cyber-crime and investigation techniques, international law, and organisational security. After studying at the FBI National Academy in Quantico, Virginia he became the founder and Head of The Computer Crime Unit New Scotland Yard from 1984 to 1996, an operational specialist unit and the forerunner of the National Hi-Tec Crime Unit and the e-Crime Unit. He was the first Chairman of the Interpol Computer Crime Committee, from 1990 to 1996, which was responsible for the worldwide standardisation of Police procedure and international training in the area of cyber-crime investigation and digital forensics. He was the 2003/4 President of the U.K. Chapter of I.S.S.A. (Information Security Specialists Association).