Corbett Paper

No 19

Some Principles of Cyber Warfare

Using Corbett to Understand War
in the Early Twenty–First Century

Richard M. Crowell

KING'S College LONDON
University of London

Some Principles of Cyber Warfare
Using Corbett to Understand War in the Early Twenty–First Century

Richard M. Crowell

Key Points:

Corbett's theory of maritime warfare is used to illustrate how forces that move through cyberspace, content and code, have similar characteristics to forces moving through the maritime domain: fluidity of movement, omni–directional avenues of approach and the necessity to make shore (reach a human or machine destination) to be useable.

- The relationship between the information environment (IE) and cyberspace as a key part of information-age war is described with a particular focus on how decision-making and control of machines takes place at the nexus of the dimensions of the IE.

- The use, and rapid adaptation of, cyber force to influence human decision-making and compel machines to work independent of their owner's intent is explored.

- Cyberspace and cyber warfare are defined in ways that provide commanders, subordinates, and political leaders with a common framework.

- Principles of cyber warfare are presented with examples from recent conflicts to illustrate the concepts of cyber control, cyber denial, and disputed cyber control.

Dick Crowell is an associate professor in the Joint Military Operations Department at the US Naval War College. He specializes in information operations and cyberspace operations. A retired US Navy pilot, he served at sea and ashore for thirty years. He is a senior associate of the Center on Irregular Warfare and Armed Groups (CIWAG) and founding member of the Center for Cyber Conflict Studies (C3S).

Common Acronyms

APT – Advanced Persistent Threat

C2 – Command and Control

C4ISR – Command, Control, Communications, or Computers, Intelligence, Surveillance and Reconnaissance Systems

CYOP – Cyber PSYOP (psychological operations)

DDoS – Distributed Denial of Service

DIB – Defense Industrial Base

DIME – Diplomatic, Informational, Military and Economic (levers of national power)

EMS – Electro-magnetic Spectrum

GPS – Global Positioning System

GUI – Graphic User Interface

IE – Information Environment

ICS – Industrial Control System(s)

ICT – Information Communication Technology

Some Principles of Cyber Warfare
Using Corbett to Understand War in the Early Twenty–First Century

Richard M. Crowell

…no one will deny that since the great theorists of the early nineteenth century attempted to produce a reasoned theory of war, its planning and conduct have acquired a method, a precision, and a certainty of grasp which were unknown before.
— Corbett, Some Principles of Maritime Strategy

Part One: Cyberspace as an Additional Field of Action for Mankind's Inevitable Conflict

Introduction

Mankind's natural state is to be competitive, which inevitably leads to conflict. Discussing the certainty of war, Albert Einstein argued, "So long as there are sovereign nations possessing great power, war is inevitable. That is not an attempt to say when it will come, but only that it is sure to come."[1] When mankind's interests took to the air General Giulio Douhet observed, "Aeronautics, opened up to men a new field of action, the field of the air. In so doing it of necessity created a new battlefield; for wherever two men meet, conflict is inevitable."[2] In his magnum opus, *On War*, Clausewitz, the nineteenth century military theorist and practitioner discussed war on a more personal level but still found war inevitable, "War is an act of human intercourse…it is part of man's social existence."[3] The inevitability of war remains regardless of the field of action.

Since the Treaty of Westphalia, war has come to be defined as state–directed force to achieve political ends. Clausewitz asserts that, "War is thus an act of force to compel our enemy to do our will."[4] He states that war is "…a paradoxical trinity – composed of primordial violence, hatred, and enmity, which are to be regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason alone."[5] This trinity of concepts is primarily represented, respectively, by the people, the military, and the government – the three historical objects of physical force. *On War* was written in the industrial age, when the force used to compel an enemy to do your will was first and foremost physical. In that age, armies principally engaged in corporeal clashes as immature means of transferring information largely prevented the concurrent influence of populations and governments. Prodigious change has occurred since then. The two original domains of war, land and maritime, have been supplemented by two additional domains, air and space. As the industrial age gave way to the information age, the quantity and speed of information transfer grew, as did its penetration into society. This evolution resulted in physical force being supplemented by additional forces – content and code (information and computer software) – that can influence all three elements of Clausewitz's trinity nearly instantaneously and simultaneously. These changes also legitimized the medium through which information moves, cyberspace, as the fifth domain of warfare.

The term cyberspace was popularized in the second half of the twentieth century in both the academic sciences and science fiction. The term was born as humans realized they needed to efficiently control the machines they created to solve problems and began to imagine the future of their

relationship with these machines.[6] The root of the word is, cyber – from cybernetics, the science of communications and automatic control systems in both machines and living things; it comes from the Greek kubernētēs - 'steersman'.[7] The image of an ancient mariner with a hand on the tiller paints the picture of control and communication in an early machine – a sailboat – highlighting key aspects of the modern term. Fast forward to modern machines, particularly ones used in information–communication technologies (ICT), and one can see the value of deliberately controlling both machines and communication in contemporary warfare.[8] The ability to manoeuvre in cyberspace in pursuit of military objectives and political ends is an increasingly important aspect of both military and national power.[*]

The use of cyberspace in the late twentieth to early twenty–first century has precipitated interest by civilian and military leaders in the study of warfare in cyberspace. However, there have been relatively few works that develop a theory for how cyberspace operations may be used in the art and science of planning, preparing, and conducting military operations and campaigns in order to compel an enemy to do one's will. Instead, much of the discussion on cyberspace operations has been focused on defensive cyberspace operations: cyber security, information assurance, and network defense. This is in part due to the faulty perception that any discussion on offensive cyberspace operations must be highly classified. In truth, it is possible to have a constructive unclassified discussion on manoeuvreing in cyberspace in support of military objectives and political ends.

That discussion should start with an open exchange of ideas on a theory of cyber warfare. Mankind's opposing interests and goals have meant that past manoeuvreing through physical domains in pursuit of resources, trade and the transfer and exploitation of information led to competition and conflict, often resulting in war. Study of warfare, particularly military theory, has led to a mature understanding of these domains. Development within the new domain of cyberspace has followed the same trajectory – discovery and development leading to competition, conflict and war – but the mature understanding of its essentials is still lacking and so requires the same attention and development of theory.

It is essential that the theory of cyberspace should include principles, which address the intertwining of cyberspace with human activity, how manoeuvreing through cyberspace can be instrumental in achieving objectives and particularly how cyber force (content and code) may be used in pursuit of victory. In each of these, the genius of Corbett's maritime concepts provide illumination, and the foundation for exploration of how the explosive pace of recent electronic innovation leads to rapid adaptation of ICT, including social media, for use in conflict.

Recent conflicts (2008 to 2016) have seen authoritative governments endeavor to control the free flow of information by attempting to control cyberspace. Their control sought to limit freedom of action but was often successfully disputed by actors who could rapidly adapt existing ICT. All of these developments require study. The accelerated intertwining of cyberspace and human activity in recent decades has given rise to both a new domain and a new form of warfare, which demands understanding by both civilian and military leaders. A theory of cyber warfare is necessary to aid leaders in normalizing their understanding of how cyberspace is used to pursue military objectives and political ends.

[*] For the purposes of this paper manoeuvre is defined as carefully guiding or manipulating someone or something to achieve an end. (Oxford English Dictionary, 11th Ed)

The monograph is divided into eight parts. The introduction describes cyberspace as an additional field of action for mankind's inevitable conflict. Part two defines cyberspace as a domain and discusses parallels to the maritime domain. Part three presents maritime warfare theory to appreciate the significant relationship between the theory and praxis of war.[9] It discusses the changes in the security environment that drive the need for a theory of cyber warfare. Fourth, the paper discusses force adaptation and rapid adaptation to illustrate how rapid adaptation of cyber force can impact modern conflict. In part five cyber warfare is defined and discussed in relation to the changing character of war. It is proposed that cyber power will only grow in importance with respect to both military and national power. Part six presents the concepts of cyber control, cyber denial, and disputed cyber control as ways of manoeuvreing in cyberspace. The seventh part presents some principles of cyber warfare to illustrate how cyber warfare has played out in in twenty–first century war. Finally, part eight draws conclusions as to the role of cyber warfare theory in contemporary conflict.

Part Two: Cyberspace as a Domain

Cyberspace, like the sea, is a field of human activity. Geoffrey Till, naval historian and Professor of Maritime Studies in the Defence Studies Department of King's College London, tells us mankind took to the sea for a variety of reasons that are linked to the attributes of the sea itself – resources, means of transportation, and a medium for the spread of information and ideas, and dominion.[10] Similarly, the Internet was created for the free flow of information and ideas. Mankind built the machines necessary to communicate and control both technologies and the electromagnetic spectrum (EMS) creating what we now call cyberspace. Manoeuvreing through it allows humans to achieve objectives, send and receive information and as with the other domains mankind attempts to achieve dominion over it. Like the sea, human use of cyberspace has expanded to include commerce and trade, and naturally mankind's use of it has evolved to include competition for control and denial.

The US military defines cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[11] This does not include the EMS, which is not man-made, yet is necessary for the physical movement of code through the domain; it also fails to recognize human use.

As humans have continually adapted tools and technology for daily use and war, to achieve their objectives more efficiently , a definition that incorporates both technology and human use helps us to begin understanding cyberspace and how to manoeuvre in it in peace and war. Daniel T. Kuehl, the former Director of the Information Strategies Concentration Program at the National Defense University provides such an inclusive definition.

> Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the *use of electronics* and the electromagnetic spectrum *to create, store, modify, exchange, and exploit information* via interdependent and interconnected networks using information-communications technologies (ICT).[12] [Emphasis added]

What moves through cyberspace is information in the form of code (software) that gets displayed as content on a graphic user interface (GUI). Therefore understanding cyber warfare begins with comprehending the Information Environment (IE). The IE is a term of art described in US Joint Doctrine for Information Operations as, 'The aggregate of individuals, organizations, and systems that collect process, disseminate, or act on information. This environment consists of three interrelated

dimensions that continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive.'[13] The continuous intertwining of cyberspace and human activity means that the dimensions of the IE are inextricably linked, resulting in cyberspace operations increasingly used to manoeuvre in support of both civilian and military objectives.

Figure 1 shows how cyberspace knits together the dimensions of the IE enabling both communication and control. It highlights how machines are used to enter cyberspace and move content and code between humans and machines with the goal of getting them to act in your favor.

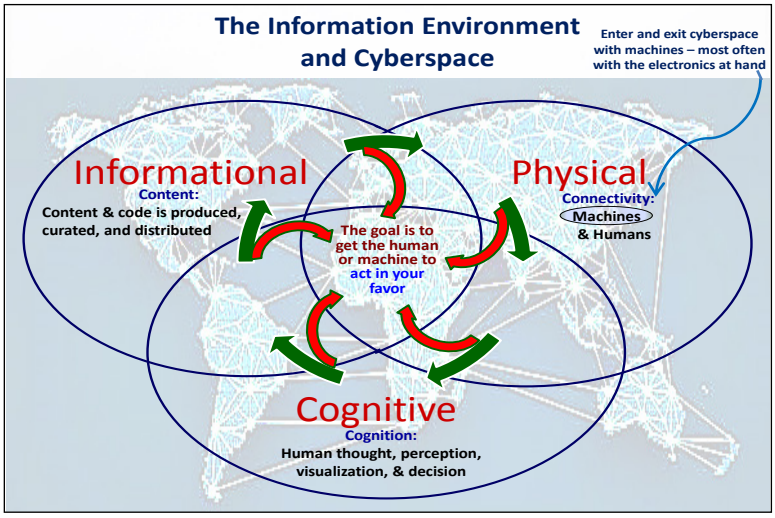

Figure 1. A representation of the information environment and cyberspace.[14]
Note: With wireless connectivity cyberspace may be ubiquitous.

The informational dimension represents the places and means by which content and code are produced and curated. It denotes *content* that is sent to humans and machines; varying widely from the spoken word to information displayed on anything from a piece of paper to a GUI or the code necessary to run machines. The physical dimension represents *connectivity* of both machines and humans (physical infrastructure and human interaction). Machines are produced to ease human work and today electronic ones are often used to distribute content that supports decision–making.[15] Electronics are generally easy to understand as they are deliberately made to be user friendly. Most people can learn to use a smartphone in about an hour, for example. Human connectivity is considerably harder to understand as learning a language or a culture takes significantly longer. The cognitive dimension represents *cognition* – human thought, reason, and decision–making; it is the most complicated because it is extremely challenging to truly know what humans are thinking.

Today communication and control happens largely via cyberspace. Grasping how cyberspace is used to move between the dimensions to access both humans and machines will help contextualize the role of cyber warfare in future conflict. The nexus of the dimensions of the IE is where humans and machines come together receiving information to make decisions and execute control. In conducting operations across the spectrum of conflict nations and militaries must both defend and use *content, connectivity, and cognition* in support of objectives and ends.[16] Cognition is arguably the most important as the decision to go to war and to end remains uniquely human. Understanding the interaction of the human and machine that occurs at that nexus will be a significant part of winning future conflict.

Some of the central challenges in understanding cyberspace relate to the speed and propagation of content and code used to achieve objectives and also to the way that machines are continuously invented and adapted for daily use and conflict. War in all domains involves relationships between time, space, and force that practitioners must balance to obtain freedom of action. These interactions apply to cyberspace as well, albeit often with different ratios than traditionally thought to achieve control. Once cyber control is obtained the controller has freedom of action to achieve objectives in cyberspace. Cyber control may then lead to freedom of action in the physical spaces by controlling machines independent of the owners or affecting adversary decision–making.

Cyberspace is the most universal of all the domains, allowing vast amounts of communication to take place electronically. Global Internet access reached more than half the inhabitants of Earth in 2015, with two-thirds coming from the developing world and three of the top social messaging sites Facebook, Twitter, and WhatsApp combined reaching billions of people.[17] Cyberspace is the only domain which all military services and branches of government rely on for daily operations. The US Department of Defense (DoD) operates more than seven million networked devices and 15,000 network enclaves.[18]

A substantial amount of the increased civilian use of cyberspace is related to the ways modern economies use data. The rise of the market–state supported by market driven economies and the continued existence of command economies both need massive amounts of data to prosper. Market–states depend on international business to create stability in the global economy.[19] Market driven economies and command economies both require cyberspace to move data. The intertwining of cyberspace and twenty–first century commerce is epitomized by the energy and financial industries use of both cyberspace and machines to ease workloads. Much of the energy industry uses industrial control systems (ICS) to pump, move, store, and consume their products. A second example of economic dependence on cyberspace is the way both market and command economies use machines for electronic fund transfers (EFT).[20] EFT's are the backbone of modern trade with electronic commerce transferring trillions of dollars around the globe daily. Cyberspace has become the life blood of modern societies.

Cyberspace is clearly a complex field of human activity – one which requires successful manoeuvreing through for much of daily life. As so much of human life is entwined with cyberspace, we must understand past cyber events, what future adversaries are learning from the deliberate input of malware (malicious software / code) into machines, and how these occurrences may shape future war. Chaos can be created with the insertion of malware into electronic systems, a power company's ICS, military command, control, communications, or computers, intelligence, surveillance and reconnaissance (C4ISR) systems. This could shut down or destroy a power grid supporting military command and control (C2) systems, resulting in an impotent military. A cyber attack against a civilian power grid during extreme cold weather could severely threaten the civilian population. While this does not fit the traditional concept of a weapon of mass destruction or effect (WMD/E), it would likely have the same effect.[21]

There are parallels between nineteenth/twentieth century national activities at sea and twenty–first century national activities in cyberspace. Throughout history commerce prevention has been realized by striking at maritime trade, the life blood of a nation.[22] Present–day adversaries have the ability to pressure their opposition's life blood in cyberspace. Maritime warfare theory can aid in our study of the evolving concept of cyber warfare.

Part Three: Maritime Warfare Theory

War at sea is a fight between all kinds of naval forces – not just capital ships.
— Stepan Osipovich Makarov, Vice Admiral, Imperial Russian Navy

Theory should be the study of war, not doctrine; it is meant to explore the nature of the ends and means of how force is used to achieve victory.[23] Milan Vego, Professor of Joint Military Operations at the US Naval War College, reasons that theories of warfare are intended to explain the nature, character, and characteristics of war in each of the physical domains.[24] He goes on to list the impact of social factors on the conduct of war, specifically ideology, science, and technology as tenets to be analyzed.[25] Theories of war are intended to normalize our understanding of the many and varied aspects of war, yet many military officers often either fail to value or outright mistrust military theory.[26] Many also condemn theory and stress the use of technology to win wars.[27]

The similarities between the sea and cyberspace suggest using maritime warfare theory to help us to begin understanding cyber warfare. Sir Julian Corbett the noted British historian and maritime theorist reminds us that understanding theory increases the effective power of conduct.[28] He stresses the importance of naval power and the relationship between the army and navy – actions and objectives ashore.[29] Corbett poses the questions of what a Navy can enable a nation to do and what the Army wants to do; thereby reinforcing the need to recognize how all actions in war play out in the land domain where humans live.[30] In addressing the interactions between the maritime and land domains, Corbett was in the early stages of thinking about what would become joint and combined warfare. Corbett discusses the concept of command of the sea (sea control),

> The object of naval warfare must always be directly or indirectly either to secure the command of the sea or to prevent the enemy from securing it. The second part of this proposition should be noted with special care in order to exclude a habit of thought, which is one of the commonest sources of error in naval speculation. That error is the very general assumption that if one belligerent loses command of the sea it passes at once to the other belligerent. The most cursory study of naval history is enough to reveal the falseness of such an assumption. It tells us that the most common situation on naval war is that neither side has the command; that the normal position is not a commanded sea, but an uncommanded sea. The mere assertion, which no one denies, that the object of naval warfare is to get command of the sea actually connotes the proposition that the command is normally in dispute.[31]

He goes on to say,

> If the object of the command of the sea is to control communications, it is obvious it may exist in various degrees. We may be able to control the whole of the common communications as the result either of great initial preponderance or of decisive victory. If we are not sufficiently strong to do this, we may still be able to control some of the communications; that is, our control may be general or local.[32]

Maritime trade warfare is an integral part of war at sea. Its goal is to weaken the military economic potential of an adversary by conducting operations throughout the entire spectrum of war at sea.[33] Actions against trade moving at sea in order to affect events ashore have been conducted since mankind first started using the sea for its resources and as a means of transportation. One of the

earliest recorded examples comes from the Peloponnesian War. Greek historian Thucydides tells us the First Sicilian Expedition was sent to "prevent the exportation of Sicilian grain to Peloponnesus."[34]

Maritime trade warfare's heyday was in the two world wars of the twentieth century. During both wars, Great Britain and her allies fought against attempts to strangle the island nation economically by conducting maritime trade warfare. Great Britain's geography meant the North Atlantic maritime trade was the linchpin of British society. Germany needed to deny the Allies control of the seas to prevent vital trade reaching Great Britain. The Allies effectively disputed German actions at sea in both wars. A World War Two illustration comes from 1939 to 1942 when German U–boats had freedom of action in the North Atlantic, sinking nearly 5000 allied ships.[35] Between 1943 and 1945 the Allies were able to decrease the size of the uncontrolled sea known as the 'black hole' in selected sea lines across the North Atlantic through the coordinated use of aircraft, RADAR, anti–submarine warfare, and signals intelligence (SIGINT). The result decreased shipping losses to about 1100 for roughly the same time period.[36] Additionally, Allied sea control and denial kept a significant part of the German surface navy and merchant fleet in port. This in turn had reciprocal impact on Germany, starving them of vital resources needed to feed their nation and supply the defense industrial base (DIB).

The intertwining of cyberspace and human activity in the twenty–first century means cyberspace is a linchpin of society's collective life. It illustrates our dependence on cyberspace for resources, as the primary medium for the spread of information, and decision–making. The need to appreciate the complexity of cyberspace in peace and war will only increase as authorities drive consumers, employees, and the general populace to cyberspace for communication, work, shopping, banking, entertainment, and war fighting.

In discussing the human ability to comprehend complex systems, Jacob Bronowski, the Polish–born British polymath, contends grouping similar objects together is the basis for the way we think.

> The action of putting things which are not identical into a group or class is so familiar that we forget how sweeping it is. The action depends on recognizing a set of things to be alike when they are not identical… Habit makes us think the likeness obvious… this ability to order things into likes and unlikes is the foundation of human thought… and a human ability; we trace and to some extent inject the likeness, which is by no means planted there by nature for all to see.[37]

The same methodology can be applied to the discussion here by relating Corbett's observations on the maritime domain to cyberspace. First, the normal state of cyberspace is uncontrolled; in conflict control is normally in dispute. Second, the goal is control of cyberspace; this implies that control is necessary to successfully manoeuvre in order to achieve objectives when parts of the domain are disputed. Importantly, the concept of general or local control shows that control exists in degrees. Unlike the land domain where borders exist and ground can be permanently controlled, in cyberspace one does not need to control the whole or even large sections of the domain to exploit the domain successfully. All one need do is control selected parts of cyberspace at the desired time; once control is obtained, that part of the domain becomes manoeuvre space with a concomitant freedom to act.

Maritime warfare, specifically sea control, sea denial, and disputed sea control therefore provides a foundation for understanding cyber warfare. Content and code moving in cyberspace have similar characteristics to forces moving from the sea, a fluidity of movement, omni–directional avenues of approach, and the necessity to make 'shore' (move to where the human and machines are) in order to be useable. Additionally, the ability to control or deny access, dispute control, and prevent the force

from making 'shore' for limited amounts of time (the fluidity of control) all speak to injecting the likeness of cyberspace into maritime theory as a way to comprehend the complexities of cyber warfare.

Corbett further theorizes that because mankind's life ashore is so entwined with the maritime domain, control of maritime communications by denying the use of distribution points can destroy the national life afloat, thereby enabling control of life ashore.[38] This idea leads to the aspects of Corbett's theory on commerce prevention, the importance of defense, and the function of the fleet to further or hinder military operations ashore.[39] The ideas on commerce prevention further link war to citizens and their collective life.[40] They too have application to the cyberspace domain. While Corbett's maritime theory has many applications to the cyberspace domain, it has its limitations particularly with respect to the changes in the global security setting. In all military theory, but particularly cyberspace theory, it must be remembered that the human is so important to war that enduring military theory should focus on the infinite complexity of the user rather than the latest technology.[41]

The Need for a New Theory of War

The changes in the international security environment, diplomacy, domestic politics, ideology, economics, and revolutionary advances in technology in recent history drives the need for additional theories of war to fit varying conditions and preconceptions.[42] These types of transformations drove the production of theory in the industrial age and continue to drive change today. When humans fight, weapons are invented, adapted, and employed and eventually humans get around to actually thinking about methods of better utilising these advances.

Colin Gray, British-American professor of International Relations and Strategic Studies at the University of Reading, notes that it is not uncommon for military capability to come before strategic thought.[43] This was true for the introduction of steam powered ships and the airplane. Many of the works of Corbett and other theorists were written decades after the introduction of steam powered "Men of War." Douhet's *The Command of the Air* was not written until nearly ten years after the first use of airplanes in war during the 1911 Italian–Turkish War. Historically, mankind's genius has been not just his inventions, but how the inventions have been adapted and put into practice during peace and war. From a warfighting perspective, this represents manoeuvreing to achieve military and ultimately political objectives and ends. Humans, as the deciders of when and how to go to war, naturally want to win and will take advantage of new technologies. When faced with war, successful leaders continuously identify lessons and often learn from their experiences. Part of this learning is fathoming the adaptation of technology created for civilian use to war.

In keeping with Clausewitz's idea that the aims belligerents adopt will conform to the spirit and character of the age,[44] many contemporary groups are already using cyberspace and adapting technology for their own purposes. Militaries and civilians alike now use cyberspace operations to achieve objectives with respect to communication, targeting, navigation (global positioning systems–GPS), logistics, training, education, shopping, banking, entertainment, and more. Cyberspace has driven changes in the economy and domestic politics in many nations, with social media helping change political power in North Africa throughout 2011, (e.g. @jan25voices and speak2tweet kept the world informed of events in Egypt when the government tried to control the Internet; these issues will be addressed later in the monograph). Radical ideology and political agendas are spread globally in near real time. There is an open realization that hostile code named Stuxnet influenced both machines and human decision–making and physically damaged machinery.

Several nations have formed military cyber commands and many more are investigating similar changes to government and military command organizations. Al Qaeda and its associated movements (AQAM), Anonymous, and the Russian Business Network are examples of non–state actors that use the domain for nefarious acts at will. The Islamic State of Iraq and the Levant (ISIL) desires to act like a state in many ways and is actively pursuing military style cyber capabilities. Global ICT corporations such as IBM, Xerox, Microsoft, Oracle, Sage, Verizon, AT&T, BT, Rostelecom, Fujitsu, Huawei, ZTE, and Apple all have equal access and vested interests in manoeuvreing in cyberspace to achieve corporate economic objectives. The global ICT corporations also provide much of the key connectivity necessary for governments and militaries to manoeuvre.

Militaries today rely heavily on an overabundance of machines that are interconnected by cyberspace. These range from ICS to run motors, sophisticated C4ISR systems, navigation, and integrated radar systems to precision weapons. Whether they are ships, main battle tanks or aircraft (manned and unmanned) modern weapons are highly technical objects that rely on both internal and external machines for communication and control. These represent some of the significant changes that Vego embraces as catalysts for new theory; they drive the need to think differently about warfare in the twenty–first century.

Part Four: Adaptation of Force and the Rapid Adaptation of Cyber Force

Force adaptation comes in response to changes in the ends, ways, means, and risk associated with how nations and militaries plan for and conduct military operations and campaigns. Adaptation can occur before or during conflict. The first half of the twentieth century saw some of the greatest advances in technology adapted for war. The internal combustion engine that powered automobiles was converted to power tanks and airplanes, and the wireless radio was adapted from news service broadcasts at and across the sea to command and control of military forces. After World War One the monoplanes that were developed for the civilian air transport market by companies like Boeing, De Havilland, Dornier, Douglas, Short Brothers, and Sikorsky increased the speed and payload of aircraft enabling them to be adapted to become heavy bombers. The Higgins Boat and Roebling Alligator, originally designed for oil prospecting and civil rescue work respectively, were adapted to become the US Marine Corps landing craft, vehicle, personnel, (LCVP) and the Amphibian Tractor (LVT).[45] Vacuum tubes, single side band (SSB) technology, and frequency modulation (FM) were developed by amateur and commercial radio operators to more efficiently use electricity and bandwidth.

The harnessing of radio frequency (RF) modulation for communication led to the refinement of radio detection and ranging becoming RADAR, the invention of television, and ultimately an understanding of the EMS that gave us cellular telephones, the Internet, the World Wide Web; all of which are elements of cyberspace. In nearly all these cases the technology was adapted from human use in peace to war and used to manoeuvre in domains to achieve objectives.

Some of the most significant advances in force generation today relate to how cyber force (content and code) is produced, curated, adapted, and moved in contemporary conflict. These have changed the character of war, as large traditional military conflicts have been replaced by more complex warfare in and among the people, where many of the actors have access to personal electronics that create, store, modify, exchange, and exploit cyber force. In many ways this transfer of power has diminished the clout of conventional militaries and shifted it to historically weaker states and non–state actors; ones that possess the ability to produce and easily adapt malware such as BlackEnergy, Metasploit, Neosploit, and Zeus.[46]

In attempting to counter this transfer of power Secretary of Defense Donald Rumsfeld formed the DoD, Office of Force Transformation (OFT) in November 2001 intending to transform US military capabilities and processes away from the industrial age to more contemporary ones. The work of the OFT was to be a catalyst for entrepreneurial and experimental thinking for defense policy and technology.[47] The focus of the OFT was on planning for, "irregular warfare (including terrorism, insurgencies, and civil war), potential catastrophic security threats (such as the possession and possible use of weapons of mass destruction by terrorists and rogue states), and potential disruptive events (such as the emergence of new technologies that could undermine current US military advantages)."[48] As a part of streamlining efforts in late 2006 the OFT was disestablished and its missions spread among the Office of the Under Secretary of Defense for Policy (OSDP), and the Assistant Secretary of Defense Research and Engineering (ASD R&E), the Deputy Assistant Secretary of Defense Rapid Fielding (DASD RF) and the Rapid Reaction Technology Office (RRTO).

The stated goals of the RRTO are: leverage all of the DoD science and technology base and those of other federal departments; stimulate interagency coordination and cooperation; anticipate adversaries' exploitation of technology, including available and advanced capabilities; provide input to guide long–term science and technology; exploit technology developed outside of DoD; and accelerate fielding of capabilities and concepts to counter emerging threats.[49] The original RRTO timing averaged five to seven years for the rapid adaption and fielding of new capabilities.[50] Timing has decreased to between six months and two years for high priority capabilities.[51] Despite this improvement, this extended time (six months to two years) to adapt technology for force generation is not remotely competitive with other actors and groups. Cyberspace is characterized by rapid adaptation. We have seen cyber force, code named speak2tweet, generated (idea to employment) in approximately 48 hours during the Arab Spring.

Cyber Force — Content & Code and their Role in Cyber Power

The ability to compel an enemy to do your will is the highest form of power in human conflict. Cyber power has been defined by Kuehl as, 'the ability to use cyberspace to create advantages and influence events in all the operational environments across the instruments of power.'[52] The last century of conflict shows that control of content and code moving through what we now call cyberspace can be instrumental as a means of compelling enemies, friends, and neutrals to act in one's favor. In *Cyber Power*, Joseph Nye discusses the three faces of behavioral power: Dahl's concept of getting others to do what they would not do otherwise, Bachrach's and Baratz's framing issues and agenda setting, and his own ideas on hard and soft power from command to co–optive behavior.[53] Nye's ideas on hard and soft power are explained,

> Hard and soft power are related because they are both aspects of the ability to achieve one's purpose by affecting the behavior of others. The distinction between them is one of degree, both in the nature of the behavior and in the tangibility of the resources. Command power – the ability to change what others do – can rest on coercion or inducement. Co–optive power – the ability to shape what others want – can rest on the attractiveness of one's culture and values or the ability to manipulate the agenda of political choices in a manner that makes others fail to express some preferences because they seem to be too unrealistic.[54]

Today cyberspace allows content and code to move between capitals and the general population with great speed and precision.[55]

Most recognizable is content; words, pictures, files, et al. are converted to digital data in the form of binary code (1s and 0s) by electronic machines. Content whether presented as radio, television, a web page, or any of the myriad social media can be instrumental in achieving both cognitive and physical objectives.[56] Influencing decision–making by getting someone to believe something they hear or see and then to act to your advantage is an example of content as a cognitive force. In discussing the importance of the human mind in warfare, Clausewitz reminds us of the decisive impact of psychological force.[57]

World War Two was the first highly technological conflict fought with reliable levels of electronic connectivity. Radio broadcasts, an example of connectivity, moved large amounts of content across the radio frequency portion of the electromagnetic spectrum between governments, militaries, and populations. Radio communication with the general populace played a significant role in events in 1930's Germany. The connectivity and content link between the government and the people was largely achieved with propaganda radio broadcasts to coerce and co–opt the people. In August 1933 Josef Goebbels proclaimed, 'The radio will be for the twentieth century what the [printing] press was for the nineteenth century.'[58] At the beginning of the war over 70 percent of German households had radios; this number grew steadily throughout the war.[59] The NAZI government became adept at using propaganda broadcasts to influence people to act in their favor. In 1944 *German Radio Propaganda* chronicled the use of radio in the NAZI's attempts to achieve their objectives. The authors explain the value of information content as force to coerce and compel in war, 'Words may achieve what bullets do not accomplish, because words do not kill. A ruthless and powerful man would be foolish if he killed opponents he could use for his own purposes. The dead can neither fight nor work. At best, they may be used as examples to frighten others, equally powerless, into yielding in order to keep alive.'[60]

In World War Two Europe, the Allied and Axis powers used radio connectivity to communicate with relevant portions of the population. Both sides also attempted to deny access to radio broadcasts of their enemy. In Great Britain, wireless radio licenses prohibited people from listening to German radio.[61] In Germany, Goebbels directed that radios be built with limited reception distances to prevent the populace from listening to radio programs from outside the country.[62] This was a more effective way of controlling the cyberspace of the day in support of military objectives and political ends. After listening to the content of the German radio broadcasts many people decided to act in favor of the NAZI government; these actions created freedom of action for the government. Decisions not to act, largely out of feelings of powerlessness or fear, also created freedom of action. To dispute this control, the British, and others, developed higher power transmitters to reach greater numbers of people in Germany and occupied territory.

The ability to adapt technology in conflict proved crucial in many ways in World War Two. The Battle of Britain gives us early examples of controlling machines and affecting human decisions through what we now call cyberspace. Throughout the summer of 1940 the Luftwaffe's nighttime strategic bombing of ports, industry and military targets combined mass and precision creating problems for the British.

The objective of the mass bombing was to compel the British to a negotiated peace. The Royal Air Force (RAF) was challenged to target and hit the large number of bombers sent against the many British targets. In combining British breakthroughs in radar and antenna technology with US applied research laboratories the Allies were able to network radars to anti-aircraft guns creating the Signal Corps Radio (SCR) 548.[63] The machines were so precise that the soldiers could watch the anti-aircraft

shells meet the incoming bombers in mid-air and destroy them.[64] The linking of man and machine could more efficiently target and kill enemy bombers than mankind alone.

In what was to become known as the Battle of the Beams – a series of scientific intelligence efforts linked to Enigma decrypts, skilled interrogation of downed German pilots, and reverse engineering of electronic gear found in aircraft wreckage determined that the Luftwaffe was using an early form of precision bombing by flying along beams that used frequencies near 30 MHz.[65] Bombers would fly outbound on a beam emanating from northern Germany until they intersected a second signal usually coming from the Low Countries, Denmark, or Norway. The pilots would begin a combination of timing and course changes (accounting for wind and groundspeed) that brought the aircraft to its intended target with great accuracy.

R. V. Jones, the first scientist assigned to the Air Ministry and his team was able to adapt American Hallicrafter S-27 amateur radio receivers, with a range from 27 to 143 MHz, to Avro Anson aircraft to determine the exact frequencies the Germans were using.[66] Further study showed that the British could not initially produce emitters with enough power to fully jam the German beams. Upon concluding that the German pilots were flying overlapping blunt signal lobes by listening to a series of dots and dashes, Jones developed a theory that he could interlace synchronized British dots and dashes to "bend the beams" and take the aircraft off target.[67] However, there was not enough time for the British to develop a system to fully synchronize their dots and dashes with the German ones.[68] Still, the chance ability of machines influencing human decision–making proved invaluable. As the aircraft approached England the German pilots heard the louder British dots and dashes and steered toward them, taking themselves off course.[69] The Battle of Britain demonstrates the ability to adapt machines to do what humans alone cannot and to control the EMS sending information that affects human decision–making. Today digital radio frequency memory (DRFM) modulators are able to control the EMS and produce a number of complex false targets that effect both machines and human decision–making.[70]

Code is used in various ways to influence decision–making. It can be written to get machines – computers, smart phones, tablets, and other forms of hardware to act autonomously. Once code has infected machines various levels of control can be gained. At the tactical level we have seen malware that allows government forces to monitor opposition forces and gain intelligence and targeting information.[71] Code is often unwittingly added by an owner who is the victim of cognitive manipulation – a phishing scheme that sends just the right content in an email convincing the owner to click on the malicious link. Manipulation of decision making can also play out with global positioning system (GPS) spoofing. A technique where hackers insert false signals into GPS to trick both machines and humans into thinking nothing is wrong as they follow the new course induced by the hacker[72] – not unlike the Battle of the Beams. While movement through the dimensions of the IE has been used for deception throughout history, today cyberspace enables deception operations to reach many more targets.

Cyber PSYOP (CYOP) is defined as cyber operations that use a computer chip aimed at directly attacking and influencing the attitudes and behaviors of soldiers and the general population.[73] CYOP enables infinite – yet accurate reach in the form of precision guided messages (PGMs).[74] The continued intertwining of cyberspace and human activity means that cyber enabling all information–related capabilities (IRCs) empowers them with precision and reach to become effective cyber warfare weapons.[75]

The November 2014 cyber-attack on the Sony Corporation is an example of controlling computer chips to directly influence decisions. Sony was hacked over the scheduled December release of *The Interview,* a fictional comedy film about an attempt to assassinate Kim Jong-un the leader of North Korea. North Korea used illegal cyber-attacks to steal and destroy data that was then used to intimidate and coerce Sony, several movie theater chains, and the American people, ultimately disrupting free speech within the United States.[76] The "Guardians of Peace" hackers reportedly stole some 100 terabytes of data from Sony servers.[77] CYOP was used to coerce Sony executives into cancelling the release the film. Sony feared further attacks could cripple the movie industry by a loss of confidence from cyberspace operations and physical attacks. It is estimated the cancellation cost Sony in excess of 100 million dollars.

Combining content and code can have synergistic effects. At the strategic level malware named Stuxnet was identified in 2010 as being able to physically alter and degrade Iranian nuclear processing equipment. Stuxnet affected both the machines and human decision–making in that it made the equipment produce substandard material and damaged machinery while giving signals to the human operators that the equipment was working well. Combining the forces of content and code allows Nye's three faces of power to play out around the world daily; issues are framed, agendas are set, people do what they would not otherwise do, command is executed, and humans and machines are co–opted. The vast increase in Internet connectivity in the early twenty–first century drives the need to recognize how the speed of movement and depth of penetration of these types of force will enable the control of machines and impact decision–making.

Part Five: Cyber Warfare

The movement of contemporary conflict from large scale army vs. army conflicts to small wars has challenged Western militaries' understanding of conflict in a multi–polar world.[78] Governments and militaries have attempted to study contemporary conflict by labeling it asymmetric, unconventional, hybrid, compound, and so on. Today's wars are fought using the characteristic weapons of the age; with belligerents and weapons increasingly interconnected by cyberspace. Cyber warfare is essentially about how cyberspace actions are used to achieve objectives and influence decision making in all domains and here maritime theory helps us to begin understanding.

The universality of cyberspace makes appreciating the relationship between the nature and character of modern war essential for both laymen and practitioners. The nature of war is constant and ageless while the character of war is malleable based on the era and technological advances of the day. While the US War for Independence was fought with soldiers, sailors, marines, muskets, long rifles, cannon, cavalry, and ships of sail and World War Two was fought with soldiers, sailors, airmen, marines, tanks, amphibious shipping, landing craft, aircraft carriers, battleships, airplanes, V–1 and V–2 rockets, and nuclear weapons, they were both wars. These conflicts illustrated the nature of war with the application of force in three traditional ways. Some were purely physical, some were psychological, but most were combined, i.e., the Colonists' use of the long rifle specifically to shoot British officers and the German use of V–1 and V–2 rockets against the population both having destructive and terror affects on the people, military, and government of their adversary.

Through the technological advances of the day the two conflicts illustrated the changing character of war. The musket, in service in nearly all European armies, was adapted by the Colonists to a rifled barrel to hunt in the vast open spaces of North America. The V–1 and V–2 rockets were largely made possible by the study of physics in the twentieth century. In these wars, like nearly all others,

mankind combined the nature and character of war to develop new and unimaginable ways to compel the enemy. We now have a similar opportunity to study the character of future conflict and to learn to use and adapt cyber force.

As war is undeniably part of man's social existence, it is natural that humans employ tools characteristic of the age in which they live. The challenges Western militaries experienced in understanding the more complex forms of warfare in early twenty–first century conflict point to the necessity of understanding both the nature and character of war, particularly how cyber warfare will be instrumental in future wars, before they begin. Understanding the accelerated use of weapons systems as interconnected machines, how information is moved to human decision–makers and how that content compels them to act will be important aspects of twenty–first century conflict. Winning future wars will require a balanced understanding of the nature and character of war.

Interestingly Sun Tzu defined the concept of communicating ground in the 4th Century BCE as battleground which is equally accessible to both adversaries.[79] Though there were no electronics in his day, there was an IE in which the connectivity and content link was the spoken and written word that influenced human cognition and action. Sun Tzu's communicating ground relates to the three dimensions of the IE. Sun Tzu clearly understood that he and his soldiers had equal opportunity to influence friends, foes, and neutrals in war and peace. Cyberspace is communicating ground open to billions of people due to the low cost of access. Sun Tzu stressed the importance of paying particular attention to defenses when dealing with communicating ground.[80]

Corbett tells us of the rewards gained by deadening the activities of an enemy at sea as a legitimate way to apply pressure.[81] The extent to which modern life depends on cyberspace operations means that the defense of nations and the collective life of the citizenry depend on the prowess and timing of defensive cyberspace efforts. We must understand the relationships between twenty–first century commerce and defense, how to use cyberspace operations to support diplomatic efforts, and most importantly how cyberspace operations may be used to further or hinder operations in all domains. The relationships between corporations, banks, telecommunications companies, the DIB, DoD, and Department of Homeland Security (DHS) and how these organizations interact electronically via cyberspace make Sun Tzu's ideas on communicating ground as relevant today as when they were written.

Industrial control systems in modern weapons systems, the DIB and EFTs are part of the twenty–first century communicating ground. The commerce aspect of Corbett's theory is important because it intertwines war with the human need to receive goods and supplies that move through the maritime domain. The commerce that moves through cyberspace comprises the code to run machines, critical infrastructure, and EFTs; these may be decisive in future wars and must be defended.

The ubiquitous labeling of all things 'cyber' drives the need for a comparison of DoD and civilian ideas on cyberspace. The following military definitions have a common thread in that they discuss how to achieve objectives. An objective is the purpose of one's actions carried out within a specific space and time; a military objective is one whose control, defense, destruction or neutralization would result in a definitive military advantage.[82] Cyberspace Operations are the employment of cyber capabilities where the primary purpose is to achieve military objectives in or through cyberspace.[83] Cyber Warfare has been defined by the US DoD as an armed conflict conducted in whole or part by cyber means; military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict; it includes cyber–attack, cyber defense, and cyber enabling actions.[84]

The intertwining of cyberspace and daily life with electronic machines monitoring of everything from home appliances and security systems to driverless cars has coined the phrase *the Internet of Things*.[85] Accordingly, the following definition of civilian cyberspace operations is presented,

> Actions that use machines (i.e., smartphones, laptops, tablets, and PCs) and cyberspace for decision–making and to achieve objectives in the physical domains. Actions include, but are not limited to, network operations for the purpose of communication, navigation, news, shopping, banking, entertainment, social–networking, data manipulation, espionage, theft, and defense of personal and non–government electronic systems.

The major issue with the US DoD definition of cyber warfare is that it confines outcomes of the military operations to *denying an opposing force the effective use of cyberspace systems and weapons in a conflict*. It neither defines *opposing force* nor recognizes the nearly equal access to the domain by the myriad of potential adversaries. Both state and non–state actors clearly have the ability to conduct warfare in the domain. It also does not address the vulnerability of civilian and corporate actors that have significant interests in the domain. Low entry costs to cyberspace allow many of the actors listed earlier to play on the same field as traditional militaries. Belligerents in future conflicts will likely not limit their actions to denying only an opposing force effective use of cyberspace. They will very likely use cyberspace to deny all elements of power: diplomatic, informational, military, and economic (DIME) use of machines and the EMS necessary for daily life. Additionally, the limited DoD view speaks only to denying an adversary use of *cyberspace systems and weapons*.[86] Keeping in mind the DoD definition of cyberspace presented earlier includes neither the EMS nor human use of the domain in its characterization.

Similarly the definition of cyber warfare does not allow for a commander to use cyberspace operations to achieve objectives broadly across all of the domains. Commanders that use airplanes or ships solely to achieve objectives in the air or at sea, ignoring objectives ashore may win battles, but not wars. Therefore, the following definition is presented,

> Cyber warfare is defined as operations in all domains to control machines or portions of the electromagnetic spectrum in order to affect decision–making to achieve significant advantage, objectives, or victory over an adversary in conflict.

This definition shows the universality of the domain and recognizes that actions in cyberspace play out in all domains. It does not limit actions to purely military forces, thereby recognizing the near equal access to cyberspace by any actor desiring to use it, and the potential effects of control or denial on any and all national activities. Control of machines permits them to work independently and control of both machines and the electromagnetic spectrum enables cognitive manipulation.

The concept of equal access recognizes that some states have a loose confederation of non–military cyber actors, as proxies, willing to conduct cyber warfare on behalf of their allied state. The US House of Representatives and the Homeland Security Policy Institute at George Washington University (GWU) reported on the Islamic Revolutionary Guard Corps (IRGC), Quds Force and Hezbollah history of acting as proxies of the Iranian government and attacking US forces and interests abroad.[87] The report stated, 'There is little, if any, reason to think that Iran would hesitate to engage proxies to conduct cyber strikes against perceived adversaries.'[88] There is also no reason to think cyber–attacks will be limited to US interests abroad.

Due to the challenges in determining attribution for certain cyberspace operations, non–military actors may have major impact on future conflict. Future cyber warfare may be state–directed force to achieve political ends, but clearly determining the identity of that state may be difficult. The challenges in determining attribution are summed up by the authors of the joint Congressional and GWU report, 'Smoking keyboards are hard to find.'[89]

Part Six: Cyber Control, Cyber Denial, and Disputed Cyber Control

> *This malware can be used to shut down vital infrastructure like oil and gas pipelines, power transmission grids and water distribution and filtration systems.*
> — Admiral Michael Rogers, USN, Commander, U. S. Cyber Command and Director, National Security Agency – Testimony to House (Select) Intelligence Committee on Cybersecurity Threats: The Way Forward, November 20th 2014

While there are many today who say cyberspace cannot be controlled, similarities in Corbett's concepts provide ways to understand control and denial in the cyber domain; control to a certain degree and for focused time and in a given space. Control of the sea historically has been about controlling a given space over a period of time needed to move forces, commerce, or trade between points or ashore. As the normal state of cyberspace is uncontrolled, the object in time of conflict is control that is necessary for manoeuvreing to gain access to decision–makers or machines. The requirement to gain control of cyberspace actually confirms that control is normally in dispute. Cyber control is a positive objective defined as *control of designated aspects of cyberspace for a specified time necessary to move the cyber force to the objective, either a machine or human decision–maker.* It will likely set the stage for offensive operations in all domains in future conflict. Cyber denial is a negative objective and is defined as, *the ability to deny use of selected aspects of the domain for the time necessary to prevent the movement of cyber force to the objective, either a machine or human decision–maker.* Disputed Cyber Control is defined as *the near constant struggle for control of cyberspace that may occur in conflict*.

The intertwining of cyberspace and human activity means nearly all future military operations will need to achieve cyber control or cyber denial prior to or while conducting operations. From a military perspective, the objective of the cyber control and/or denial should be linked to achieving the operational commander's objectives. These objectives may be physical or cognitive, i.e., the ability to communicate, use electronic machines, conduct a deception operation (the sowing of distrust), or denying electronic sensors to the adversary.

In, *World War, The Third World War – Total Information Warfare,* Shen Weiguang, states that the main task [of Information Warfare] should be 'disrupting the enemy's cognitive system and its trust system.'[90] If a commander loses trust in the force's machines or fails to properly employ them, the adversary has won. Additionally, if a population loses faith in its government or military, the adversary has won.

The object of cyber control is the regulation of selected aspects of cyberspace, in various degrees, through the judicious movement of code and or content. Cyber control in support of objectives in all domains is limited to specific space and time. Denial of vast amounts of cyberspace for long periods of time may be possible with certain decisive action (i.e., an electromagnetic pulse burst). If there is not sufficient strength to do this, cyber denial or control will likely be general or local. Often

general or local cyber control is all that is required to send or receive content and/or code to affect the human or the machine.[91]

Military cyber control can be executed by theater strategic, operational, and tactical commanders and is meant to create the conditions that enable tactical forces to fight and win in all domains. Once cyber control is obtained, it may only need to be maintained for the time required to move cyber or traditional forces into place. If the code is sufficiently hidden, the cyber control may go unknown for extended periods of time. When activated it could provide a military advantage in cyberspace or other domain. Examples of cyberspace operations that can lead to cyber control or denial are: attack of code or content at rest in machines; accessing code or content en route to machines or humans (i.e., tapping into undersea cables); blockading or EW jamming of selected connectivity (boxes, wires, cables, or antennae); inserting malware into machines to regulate them.

Cyber control and disputed cyber control differ from sea control and disputed sea control in attribution and overtness. Control and disputes at sea will normally be done openly when belligerents are clearly at war. The challenges that adavanced persistant threats (APTs) provide in attributing cyberspace operations means the seeds of cyber control or denial may be sown covertly long before there is open warfare. APTs can reside covertly in ICS and when activated, take control of specified machines. Increasingly they are prepositioned to be used as an integral part of larger information operations to intimidate or coerce a potential opponent's decision–making.

Cyber denial, much like sea denial, requires thought on how to prevent an enemy from securing control of cyberspace for military or economic purposes. When an adversary is weaker in one or more of the physical domains of warfare, it may choose to deny cyberspace to the stronger side while manoeuvreing forces in order to obtain cyber control and/or control in one or more of the physical domains. Examples of cyber denial include malware as mining; the covert delivery of code that sits undetected in the electronics of an ICS, C2 systems, or a production line. Code can be programmed to activate on command or when a certain set of parameters are met; denying access to military and/or civilian electronic connectivity or information. Examples of distributed denial of service (DDoS) include blockade of content and/or code on governments, militaries, or commerce; Anonymous is known for this style attack on credit card companies and other corporations.[92] Cyber attacks have evolved from DDoS, which have been temporary, to the control and destruction of machines. Rogers explains in detail the ability to control machines,

> So once you're into the system and you're able to do that [harm], it enables you to do things like, if I want to tell power turbines to go offline and stop generating power, you can do that. If I wanted to segment the transmission systems so that you couldn't distribute the power that was coming out of power stations, this would enable you to do that. I mean, it enables you to shut down very segmented, very tailored parts of our infrastructure that forestall the ability to provide that service to us as citizens.[93]

Trojan horse malware named BlackEnergy (BE) capable of controlling critical infrastructure made headlines in 2014. Originally designed to create Botnets that executed the DDoS attacks on the Republic of Georgia's communication networks in the 2008 war with Russia; it has been re–designed as an APT. On 23 December 2015 BE was used to attack the Ukrainian power grid.[94] The coordinated attack on three regional electric power distribution companies (oblenergos) impacted approximately 225,000 customers. Additionally, all three companies indicated that some parts of their systems were wiped using KillDisk malware.[95] KillDisk erased selected files on the target systems and corrupted the

master boot record, rendering systems inoperable.[96] While operations were eventually restored all three oblenergos remained at a reduced operating capacity more than two months after the attack.[97]

Media reports citing DHS sources speculate the Russians may be using a play from the Cold War as malware may now be emplaced to be used as a form of mutually assured destruction (MAD) against a cyber-attack or other form of strategic attack.[98] The ability to control critical infrastructure and deny access to important information by destroying networked machines has many current and former US government officials concerned about similar attacks on relatively undefended corporate, state and local government, and national networks.[99]

Cyber control or denial by states or their proxies wishing to compel an enemy will likely be part of future wars. The North Korean attack on Sony illustrates a relationship between control and denial to coerce a decision. While North Korean cyber control was against a corporation and not an attack on the life blood of a nation their actions demonstrate that enemies skilled at adapting malware could produce more dire results in a conflict. A coordinated series of cyber–attacks to control or deny access to critical infrastructure could influence decision makers to decide in favor of the attackers.

Disputed cyber control will occur when competition for access to connectivity, content, or the EMS arises in conflict. Dispute will include industry, communication, and weapons systems due to their reliance on cyberspace for everything from operating to navigation and targeting. Disputing cyber control can limit communication between forces, both humans and machines. Disputed cyber control will normally be a key objective of the weaker force. This force may be relatively weaker in informational, military, or economic elements of power or specific domains. It can choose to dispute its opponent's use of cyberspace throughout all phases of conflict – remembering that cyber control is relative to time and space.

Future cyber–attacks may drive belligerents to negotiations that lead to decisions limiting the use of cyber or physical force. The intertwining of cyberspace with nearly all aspects of life demands we understand how cyber control, cyber denial, and disputed cyber control can lead to freedom of action in future conflict.

Part Seven: Principles of Cyber Warfare

1) *Cyber control is a positive objective that must be achieved to realize freedom of action in all domains; it is relative to time and space and much like sea control exists in degrees.*

Cyber Control in the Russia – Georgia War of 2008

During the summer of 2008 Russia was asserting its power over the Republic of Georgia in order to gain control of the disputed territories of South Ossetia and Abkakhazia. The brief conflict that was reported as lasting from 7-12 August is often cited as the first use of cyber warfare with the DDoS attacks on Georgian command, control, and communications. Cyber warfare conducted by non–state proxies was instrumental in the Russian Federation forces and local militia paramilitary forces accomplishing operational and strategic objectives.

Andro Barnovi, Georgia's Deputy Defence Minister described the operational goals of the cyberspace operations conducted against his nation as creating:

> Sense of insecurity within the society; Mistrust to government; Panic caused by misinformation; Hindering government information policy; Direct economic damage; Disorder of communication systems; Weakened coordination within governmental agencies; Dysfunction of command and control systems and subsequent direct physical damage [Sic]; Decrease of legitimacy of the government activities inside the country and abroad; Acquire reliable information about the actions and dislocations of Georgian army units and leadership.[100]

The goals of the cyberspace operations were clearly to control cyberspace to affect human decision–making. In his cyber war case study David Hollis states,

> The culmination of these trends resulted in a situation that prevented government agencies in Georgia from communicating, both locally with their population and strategically with the rest of the world. Russia was able to successfully attack … across several warfighting domains, to include the cyberspace domain through propaganda operations, and denial, disruption, and degradation of Georgian communications.[101]

Unidentified proxies controlled access to the Georgian government command and control (C2) and commercial nodes that were necessary to effectively run the government. Additionally, effective information operations, with a large amount of propaganda (content) moving through cyberspace allowed Russian forces and supporters to control the narrative. The cyber attacks were limited to specific time and space, C2 nodes, and networks. They were primarily DDoS attacks (temporary and in degrees) aimed at controlling the use of cyberspace to prevent movement of information content between Georgian President Saakashvili and his civilian and military leaders.

Cyber control was successfully employed to coerce and compel the overmatched Georgian forces to do their will. The cyberspace operations can be seen as cyber fires conducted prior to the aggressor's use of conventional forces: mechanized armor movement through the Roki Tunnel, bombing by Russian Air Forces, and naval operations in the Black Sea.[102] Cyber warfare achieved cyber control in degrees necessary to allow Russian Federation forces freedom of action, first in the cyberspace domain and subsequently in the physical domains. The control of content across multiple layers of connectivity to regional, and global target audiences had strategic implications on Georgian decision–making. The control forced them to attempt filtering their communications with regional and global allied nations' connectivity. When this failed, they sued for peace.[103] Regardless of the identity of those who conducted them, the cyberspace operations were clearly instrumental in compelling the Georgian forces to do their enemy's will.

> *2) Because cyberspace provides the ability to affect decision–making and machines, the primary function of a cyber force is to further or hinder decision–making for operations in all domains of war.*

Traditionally all levers of power are engaged to influence adversaries and potential allies to decide favorably in support of larger objectives. Cyberspace gives content and code unparalleled movement and penetration into society enabling them to increasingly influence more people. In 2011 content and code were key elements of the opposition forces across North Africa ability to influence decision-making and change governments.

Egypt

During the 2011 Egyptian revolution, President Hosni Mubarak's government forces shut down the Internet in what can be seen as an attempt at total cyber control. As the stronger side in cyberspace their objective was to prevent the protestors in Tahrir Square and other sites around Egypt from communicating with local, regional, and global audiences – influencing their decision to act. On the night of January 27–28, in what the government clearly considered a near perfect scenario, as the four major lines of communication into the country were all government controlled, régime forces ordered the Internet service providers to shut down all connectivity. Ryan Singel from wired.com stated, "[T]he shutdown made it impossible for traffic to get to websites hosted in Egypt or for Egyptians to use email, Twitter or Facebook."[104]

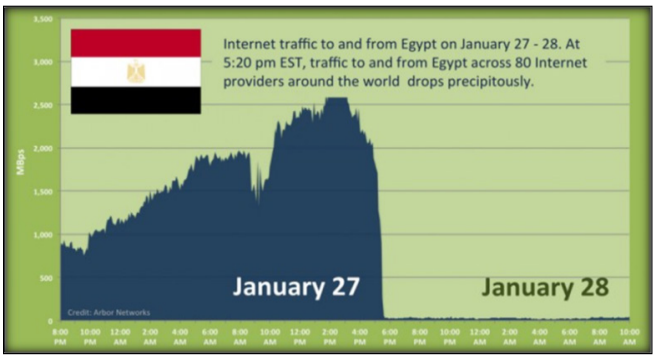

Figure 2. Arbor Network depiction of Egyptian Internet activity 27 and 28 January 2011[105]

James Cowie Founder and Chief Technology Officer for Renesys: the Internet Intelligence Authority, confirmed these reports stating,

> …every Egyptian provider, every business, bank, Internet cafe, website, school, embassy, and government office that relied on the big four Egyptian ISPs for their Internet connectivity is now cut off from the rest of the world. Link Egypt, Vodafone/Raya, Telecom Egypt, Etisalat Misr, and all their customers and partners are, for the moment, off the air.[106]

The Egyptian government attempted to use cyber control in support of their objectives to affect the decision–making of local, regional and global audiences; they failed to appreciate that it is temporary, exists in degrees, and is relative to time and space.

<u>Disputed Cyber Control – Adapting Existing Technology</u>

The Egyptian opposition successfully disputed governmental cyber control. In what can be viewed as manoeuvreing to achieve objectives, the Egyptian opposition skillfully used selective connectivity to move content; initially prompted by John Scott–Railton and @jan25voices, to dispute governmental cyber control. The use of human and limited technical connectivity via telephones (both cellular and land lines) and social media aided the Egyptian opposition in outmanoeuvring the government forces. At the outset, Scott–Railton and several friends outside Egypt understood that whatever control they could wrest away from the government would be temporary and exist in small degrees. Telephone calls were made into the country to find out what was happening. Scott–Railton then encouraged an increasing circle of friends inside Egypt to call his and other phones; the calls were recorded and the content was translated when necessary. The content was then either tweeted or posted on various

forms of social media. Realizing that faster and more accessible connectivity was needed, Scott–Railton formed @jan25voices, a network of associates who moved information content to millions of people.[107]

In a parallel effort of manoeuvreing with code, two computer scientists, Ujjwal Singh and AbdelKarim Mardini wrote the computer code to generate content as cyber force in approximately 48 hours. Initially named SayNow media, the code enabled telephone conversations to be broadcast over a Twitter feed. This rapidly evolved into speak2tweet, which was quickly purchased by Google. Google's Singh and Mardini explain their weekend work in a January 31, 2011 blog:

> Like many people we've been glued to the news unfolding in Egypt and thinking of what we could do to help people on the ground. Over the weekend we came up with the idea of a speak–to–tweet service – the ability for anyone to tweet using just a voice connection.
>
> We worked with a small team of engineers from Twitter, Google and SayNow, a company we acquired last week, to make this idea a reality. It's already live and anyone can tweet by simply leaving a voicemail on one of these international phone numbers (+16504194196 or +390662207294 or +97316199855) and the service will instantly tweet the message using the hashtag #egypt. *No Internet connection is required.* People can listen to the messages by dialing the same phone numbers or going to twitter.com/speak2tweet.
>
> We hope that this will go some way to helping people in Egypt stay connected at this very difficult time. Our thoughts are with everyone there.[108] [Emphasis added]

The Egyptian opposition, which included tech savvy innovators working from near and far, skillfully disputed cyber control, manoeuvreing with content and code to achieve cognitive objectives. The limited cyber control allowed opposition forces to produce content by narrating and eventually filming events. Opposition forces were able to use Nye's concept of co–optive power to affect decision–making. This shaped what people desired – to support the people of Egypt. The content coming from inside the country was intangible force that had an emotive effect on those who received it. European and global audiences then supported the opposition with money, connectivity, content, and ingenuity. Manoeuvreing within the existing human networks and rapidly adapting the limited technical ones allowed the opposition forces to achieve physical objectives too. They organized demonstrations, impeded government forces, and responded with counter–propaganda.

The events of the Arab Spring in Egypt clearly show how code and civilian technology were rapidly adapted for use in conflict. Cyber warfare played out as cyber control, cyber denial, and disputed cyber control across Egypt and the globe; once cyber control was achieved it enabled freedom of action in the cyber domain that went on to achieve freedom of action in the physical domains. This freedom of action ultimately allowed the opposition to achieve the physical objectives of over throwing Mubarak's regime. The Egyptian opposition's operations in the land domain clearly depended on a cyber force. Cyber forces hindered government forces and enabled opposition forces to act decisively. In Egypt cyber warfare proved a means to an end, not the end itself.

3) Cyberspace provides a new ability to interfere with any modern economy on the globe and thus influence the military–economic potential of states.

The intertwining of cyberspace and human activity means that cyber trade warfare will take part across the entire spectrum of war with the goal of weakening the enemy's military–economic potential. Just as maritime trade warfare can affect the life blood of a nation, so can cyber trade warfare. With the ever increasing amount of commerce conducted via civilian cyberspace operations, one need not stretch the imagination far to see the possibilities for cyber–attacks on ICS needed to run critical infrastructure, commerce, or a DIB.

In his 2011 paper, "The Vulnerabilities of Developed States to Economic Cyber Warfare," Paul Cornish, then Head of the International Security Programme at Chatham House, discusses the continued intertwining of developed societies and cyberspace. Cornish contends that their dependence on this connectedness, the cyber related vulnerabilities it represents, and the sovereign political structure developed in 1648 may not be the best structures to deal with the risk. He presents the concept that a large scale economic cyber attack could undermine the most important commodity of all–confidence.[109]

Highlighting that competition in cyberspace has evolved from exploitation and disruption to sophisticated influence and physical destruction, in 2014 media outlets reported on a 2008 oil pipeline explosion in Turkey.[110] The attack on the Baku–Tbilisi–Ceyhan (BTC) oil pipeline and subsequent analysis gives insight into the ability of cyberspace operations to influence the military–economic potential of states. The BTC (along with other oil and gas pipelines) was built in part to circumvent the Russian Federation's stronghold on fossil fuels from the Caucuses and Central Asia to Europe.[111]

During the summer of 2008 the BTC pipeline was on its way to reaching peak capacity with a planned goal to represent ten percent of Georgia's annual revenue.[112] On August 6th valve station number 30 near Refahiye, Turkey exploded from an over pressurization created by independent control of the machines running the pipeline.[113] Analysis of events by numerous government and corporate officials indicates that the attack combined sensor jamming, control of communication lines, along with exploitation of surveillance equipment to gain access to the network and ICS that enabled the over pressurization to occur.[114] Curiously, in the early hours of 9 August Russian jets attempted to bomb the BTC pipeline in the Gatchiani, Gardabani district, 20 kilometers south-east of Tbilisi, Georgia.[115]

A 2014 SANS case study, *Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack* analyzed publicly available information on the incident to provide a learning opportunity for ICS defenders.[116] The authors stated that while they have not confirmed the incident as happening exactly the way it was described by media reports, they conclude the cyber incident contains reasonable elements that defenders should study and exercise by superimposing the reported capabilities and techniques against their own systems.[117] The cyber and air attacks on the BTC pipeline appear to be linked to the conflict in Georgia and may well be seen as an attempt to strike Georgia's military–economic potential.

4) Effective cyber defense will be a key to forces moving to strategic offensive in future conflict.

It is likely that the first shots of the next war will be fired in cyberspace – well before kinetic ones.[118] Chinese Colonels Liang and Xiangsui frame future war as 'beyond its traditional military domain.'[119] They state that, "In warfare and non-military warfare, which is primarily national and supra–national, there is no territory which cannot be surpassed; there is no means which cannot be used in the war; and

there is no territory and method which cannot be used in combination."[120] We must be able to defend in cyberspace as we defend in other domains.

Corbett's concept of defense stresses the importance of preventing the enemy from securing use of the sea. In both the maritime struggles of the two world wars of the twentieth century Germany failed to prevent the Allies from securing use of the sea. Corbett also discusses the importance of defense by referencing both Clausewitz and von Moltke, stating the, "…the strongest form of war – that is, the form which economically makes sense for the highest development of strength in a given force – is strategic offensive combined with tactical defensive."[121] This directly supports Clausewitz' idea that, "… the natural course in war is to begin defensively and end by attacking."[122]

Both World Wars can be seen as the Allied Powers successful combining of tactical defensive with strategic offensive. Whether it is the struggle for control of the Atlantic 1914–1918 and 1939–1945, the struggle for air superiority over southern England during summer 1940 discussed earlier, or the sea denial and sea control in the Pacific theater, the Allies were able to defend tactically. The defense was just enough until a favorable balance of strength was created to enable transition to attacking with great force.

One illustration of the need for effective cyber defense concerns the DIB. The interconnectedness of modern critical infrastructure and the DIB means prudent governments must value defense, including the study of the effects code may have on the military–economic potential of their nations. In his March 2015 testimony before the Senate Armed Services Committee Admiral Rogers made clear his concerns about the persistent theft of intellectual property from government and corporate sources; noting the vast access potential adversaries have to our industrial base and critical infrastructure.[123] A key difference between the Axis and the Allies in World War Two was that when the Allies suffered heavy losses the US industrial base had the ability to replace lost combat power. Today's DIB reliance on electronics and ICS, similar to Corbett's distribution points discussed earlier, may prove to be an Achilles Heel.

Militaries employ the concept of continuity of operations with respect to C4ISR systems across the spectrum of conflict. Continuity of operations manifests as redundancy built into systems in order to ensure the man–machine interface works when needed. It is by nature costly to include multiple back–ups, but necessary to go in harm's way. The US DIB that has been protected from physical attack by two great oceans throughout our short history now finds itself vulnerable to attack through cyberspace. Does the DIB have a false sense of protection? Have they invested enough in the resilience of systems needed to run production lines or the critical infrastructure necessary for life in a modern connected society? Numerous authors have presented the concept of cyber resilience as a way of bringing continuity of operations to the DIB and other critical infrastructure. It is critical for nations to apply resilience as surprise will happen as long as cyberspace exists and machines are required to run so much of the daily lives of its citizens.[124] The heart of our military–economic power is the DIB with its modern production lines.

The DIB manufactures everything from Tomahawk Land Attack Missiles (TLAM) to F–35 Lightning II aircraft, along with shipyards that build or repair ships and submarines and perhaps most importantly include companies that produce the micro–processor chips and write the code that run the sophisticated machines. The DIB, financial, and energy sectors must incorporate resilience so that our nation can to move to a strategic offensive when required.

Part Eight: Conclusion

The enduring nature of war means that mankind's competitiveness can evolve to war at anytime and when it does the resources that are employed will come from the age in which we live. Mankind's ever-increasing desire to use machines to ease work has intertwined cyberspace with nearly every aspect of human life. More importantly modern military machines operating in all domains are highly dependent on cyberspace. The communication and control that cyberspace enables has clearly changed the character of both our lives and war. Cyber force (content and code) is now used by states and non–state actors to coerce and compel adversaries and allies in support of objectives and ends. Winning future wars will require not only building the right cyber force, but also normalizing cyberspace operations in the minds of civilian and military leadership for the planning, preparing, and conducting of military operations and campaigns. Corbett's ideas on command of the sea can aid decision–makers in understanding cyber warfare – cyber control is time and space dependent, exists in degrees and will normally be executed in support of objectives in the traditional domains. Each person in a responsible position must be educated on the basic principles and wholly familiar with cyber control, cyber denial and disputed cyber control as ways of manoeuvreing in cyberspace.

Commanders in pursuit of military objectives and political ends must learn how to gain cyber control in order to exploit it and must understand how to prevent enemies from securing the use of cyberspace. Cyber warfare's control of machines allows them to work independent of the owner's intent. Control and denial of content represent cyber power enabling issues to be framed, agendas set, command executed, and coercion and co–opting of humans. Time to adapt force can now be measured in hours compared to weeks, months, and years of the industrial age. The Arab Spring shows that content moving via cyberspace can crowdsource tangible and intangible force aiding opposition forces in overthrowing authoritarian regimes. And adapting the forces of content and code can play a significant role in contemporary conflict. The ability to adapt cyberspace capabilities faster than one's adversary will be key to controlling, denying, and disputing cyberspace.

Cyber warfare is a fight between all kinds of cyber forces – not just strategic ones; properly employed it can result in freedom of action in all domains of war. These relationships will mature as the many and varied forms of machines, and human uses of them continue to evolve. Understanding how to move from a tactical defense to a strategic offensive when cyberspace is denied or degraded will be instrumental in defending one's homeland. In developed and developing states our collective lives are so entwined with cyberspace operations it is now possible that a state's national activities in cyberspace can be deadened. We must be able to think and act defensively. Recognizing that we cannot defend all of cyberspace, we must learn what to defend, when to defend it, and how. Everyone using ICS must be able to deny the enemy the ability to secure the use of their part of cyberspace – using resilience and other defensive measures until a more favorable balance of strength is created will be key to moving to a strategic offensive.

The study of maritime theory has stood the test of time through changes from sail to steam, cannon to missiles, and the introduction of submarines and aircraft to the maritime domain. It served as a foundation to normalize cognition of how actions at sea can further or hinder actions ashore. Cyber warfare theory will strengthen the relationship between the technologists and the warfighters as they learn the risks and opportunities of networking machines to support manoeuvreing through all domains of war. Controlling cyberspace for limited time and space will prove as essential to freedom of action in the next inevitable conflict as sea control was for operations at Yorktown, Gallipoli, the Philippines, the Western Desert, Normandy, and the Falklands. Corbett's ideas on military theory endure with respect

to cyber warfare – theory enables commanders, subordinates, and their political leaders to think on the same plane.[125]

End Notes

[1] Albert Einstein, *Ideas and Opinions* (New York: Crown Inc., 1954), 118.
[2] Giulio Douhet, *The Command of the Air*, 1921, trans. Dino Ferrari. (1942; new imprint Washington, DC: Office of Air Force History, 1983), 3.
[3] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 149.
[4] Ibid., 75.
[5] Ibid., 89.
[6] For and in-depth study into how the term cyberspace came about see Thomas Rid, *Rise of the Machines A Cybernetic History,* (New York: Norton & Co, Inc., 2016).
[7] Norbert Weiner, *Cybernetics Or, Control and Communication in the Animal and the Machine* (New York: John Wiley & Sons, Inc., 1948), 19.
[8] Although cyber warfare is a new form of warfare relative to ancient forms Michael Warner argues in *Cybersecurity: A Pre-History* that the cyber issue has not just developed in the last few years, rather, it has taken decades to develop. Warner discusses US and USSR attempts to manipulate early computers and industrial control systems, what we now call SCADA, in both countries during the last two decades of the twentieth century and suggests that the media attention given to cyber topics today could easily have been written decades ago.
[9] Maritime warfare theory is a body of work concerned with the significance, development, and execution of Seapower in support of nation states political and military objectives. Some of the most prominent authors on war in the maritime domain are Sir Julian S. Corbett, Rear Admiral Alfred T. Mahan, US Navy, Geoffrey Till, and Milan Vego.
[10] Geoffrey Till, *Seapower, A Guide for the Twenty–First Century* (London: Frank Cass, 2004), 6.
[11] US Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02, Washington DC: CJCS 8 November 2010, As Amended Through 15 November 2014, 59.
[12] Daniel T. Kuehl. Cited in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Eds., *Cyberpower & National Security* (Washington, DC: Potomac Books, 2009), 28.
[13] US Office of the Chairman of the Joint Chiefs of Staff, *Information Operations,* Joint Publication (JP) 3-13, Washington DC: CJCS 27 November 2012, I-1.
[14] Venn diagram by the author. Slide background image of interconnected world obtained 11 July 2016 from US Department of State, http://www.state.gov/s/cyberissues/strategy/.
[15] Machines are tools invented to ease human work and achieve goals. Originally machines were created to ease physical work; today many machines are designed to ease mental work. Machines may be powered by mechanical, thermal, chemical, or electrical means. Today many machines use some form of electronics to control or regulate their workings.
[16] The spectrum of conflict is based on the probability of occurrence versus the level of violence. It ranges from operations occurring frequently like peacetime presence that are relatively low in violence to strategic nuclear war that occurs very infrequently but is extremely violent. Source: *The Maritime Strategy*, US Naval Institute Proceedings, January 1986, supplement 8; The concept of renaming the dimensions of the IE to the three C's of content, connectivity, and cognition comes from a brief presented by Dr. Daniel T. Kuehl from the National Defense University in 2009 and fits well with understanding content and code as a force that moves through cyberspace.
[17] *The World in 2015, ICT Facts and Figures*. The International Telecommunication Union, Place des Nations 1211 Geneva 20, Switzerland, 21 November 2016, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf ; Parmy Olsen, "These Numbers Show Facebook

Is Trailing Social Messaging Apps Globally," 4 December 2013, http://www.forbes.com/sites/parmyolson/2013/11/26/these-numbers-show-facebook-is-trailing-social-messaging-apps-globally/.

[18] Admiral Michael Rogers, USN, Commander United States Cyber Command and Director National Security Agency, *Statement of Before the Senate Armed Services Committee*, 19 March 2015.

[19] Philip Bobbitt, *The Shield of Achilles* (New York: Anchor Books, 2003), 229.

[20] Examples of EFTs include: online banking, credit card use, direct deposit of payroll, direct debit, electronic benefit transfer, electronic private currency movement, wire transfer, electronic bill payment.

[21] A weapon of mass destruction (WMD) is defined as chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. (US Department of Defense Dictionary of Military and Associated Terms (Joint Publication 1-02), 8 November 2010, As Amended Through 15 April 2013, 302). Weapons of mass effect (WME) are weapons capable of inflicting grave destructive, psychological and/or economic damage to the United States. (Homeland Security Advisory Council Weapons of Mass Effect Task Force on Preventing the Entry of Weapons of Mass Effect Into the United States, January 10, 2006, 3).

[22] Julian Corbett, *Some Principles of Maritime Strategy* (London: Longmans, Green and Co., 1911), 90.

[23] Clausewitz, *On War*, 141-142; Military Doctrine is defined as, "Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application." Joint Publication 1-02, 86.

[24] Milan Vego, "On Military Theory." *Joint Force Quarterly* (Washington, D C: National Defense University Press, 2011), Issue 62, 60.

[25] Ibid.

[26] Henry E. Eccles, *Military Concepts and Philosophy* (New Brunswick, NJ: Rutgers University Press, 1965), 24.

[27] Ibid.

[28] Corbett, *Some Principles of Maritime Strategy*, 2

[29] Ibid., 9.

[30] Ibid., 14.

[31] Ibid., 87.

[32] Ibid., 100.

[33] Milan Vego, *Study War Much More*. US Naval Institute Proceedings. January 2013, 60-61.

[34] Thucydides 3, 86.

[35] US Merchant Marine in World War Two, 22 February 2013, http://www.usmm.org/ww2.html.

[36] Ibid.

[37] Jacob Bronowski, *The Common Sense of Science* (Cambridge, MA: Harvard University Press, 1966), 27-28.

[38] Corbett, *Some Principles of Maritime Strategy*, 91.

[39] Ibid., 87-104; Corbett, *England in the Seven Years War: A Study in Combined Strategy*, Vol 1 (London: Longmans, Green and Co., 1904), 6.

[40] Corbett, *Some Principles of Maritime Strategy*, 91-94.

[41] Ryan Henry and C. Edward Peartree, *Military Theory and Information Warfare.* Center for Strategic and International Studies: Carlisle, PA. *Parameters*, Autumn 1998, 121-35.

[42] Vego, "On Military Theory," *Joint Force Quarterly*, (Washington, D C: National Defense University Press, 2011), Issue 62, 60.

[43] Colin Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld & Nicolson, 2005), 320.

[44] Clausewitz, *On War*, 594.
[45] These craft eventually gave birth to nine different types of Allied landing craft used in World War Two.
[46] These are all forms of malware that are used for control, denial, espionage, subversion, sabotage and destruction. BlackEnergy (BE) can be traced back to the cyber-attacks in the Russia – Georgia conflict of 2008. Originally designed to create the Botnets that executed the effective distributed denial of service (DDoS) attacks on the Georgian communication networks, BE and other variants have been widely adapted for use in a variety of modes from sending SPAM, to cyber-crime, and destruction.
[47] Josh Rogin, *DOD decides to Close Office of Force Transformation,* FCW The Business of Federal Technology, September 4, 2006, 16 September 2013, http://fcw.com/articles/2006/09/04/dod-decides-to-close-office-of-force-transformation.aspx.
[48] Donald O'Rourke, "Defense Transformation: Background and Oversight Issues for Congress." *Congressional Research Service (CRS) Report*, November 9, 2006, 5.
[49] Rapid Reaction Technology Office Brief, 12 September 2013, http://www.dtic.mil/dtic/stresources/researchinprogress/rrto_desc.html.
[50] Assistant Secretary of Defense for Rapid Fielding Brief, March 2004.
[51] Rapid Reaction Technology Office, Program Manager Brief, September 2013.
[52] Kuehl, Cited in *Cyberpower & National Security*, 38.
[53] Joseph S. Nye Jr., "Cyber Power." *Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School*, May 2010, 2.
[54] Nye, "Soft Power & Leadership." *Paper, Harvard Kennedy School, 2004*, 15 June 2010, http://www.hks.harvard.edu/leadership/Pdf/SoftPowerandLeadership.pdf.
[55] Throughout the twentieth century various forms of connectivity were used to move selected content to the people in support of achieving objectives and political ends; notable examples include the influence of masses using the political dogma of fascism, communism, socialism, and radical religious ideas.
[56] Examples of physical objectives are seizing a hill or destroying a headquarters building. Cognitive objectives are ones that influence individuals to act in one's favor. Information is presented in a variety of forms to convince individuals that planned actions are just. Cognitive objectives often lead to individuals acting out their beliefs in physical ways, i.e., Kamikaze pilots of WWII or suicide bombers in contemporary operations.
[57] Clausewitz, *On War*, 127.
[58] Joseph Goebbels, "Der Rundfunk als achte Großmacht," *Signale der neuen Zeit. 25 ausgewählte Reden von Dr. Joseph Goebbels* (Munich: Zentralverlag der NSDAP, 1938), 197-207.
[59] Frank Chalk, "Radio Propaganda and Genocide," 22 April 2013, http://migs.concordia.ca/occpapers/radio_pr.html.
[60] Ernst Kris and Hans Speier, *Nazi Radio Propaganda* (New York: Oxford University Press, 1944), 1.
[61] Mary Cawte, *Making Radio into a Tool of War*, 26 April 2013, http://www.bmartin.cc/pubs/peace/96Cawte.pdf, 8.
[62] Frank Chalk, "Radio Propaganda and Genocide," 22 April 2013, http://migs.concordia.ca/occpapers/radio_pr.html.
[63] Thomas Rid, *Rise of the Machines A Cybernetic History* (New York: Norton & Co, Inc., 2016), 19-21.
[64] Ibid., 21.
[65] R. V. Jones, *The Wizard War* (New York: Coward, McCann & Geoghegan, Inc., 1978), 93-105.
[66] Alfred Price, *The History of US Electronic Warfare – The Years of Innovation–Beginnings to 1946* (Westford, MA: The Association of Old Crows, 1984), 12.
[67] Jones, *The Wizard War*, 128.

[68] Ibid.
[69] Ibid.
[70] DRFM is a radar system developed in the last quarter of the twentieth century for digitally capturing and retransmitting RF signals. Initially used for jamming radars, increased computing power enabled DRFM to control the EMS to create radar scenes with high-resolution false targets. See *DRFM–Modulator for HRR–Jamming.* Oyvind Thingsrud, FFI – Norwegian Defence Research Establishment, NATO R&T Organization Paper, RTO-MP-SET-080, 2004.
[71] John Scott-Railton, "Why is the webcam on in the room with the missiles? Opposition movements and their adversaries go online," Brief to the June 2013 Naval War College, Center on Irregular Warfare and Armed Groups Symposium.
[72] Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of a UAV, Aerospace *Engineering and Engineering Mechanics, 28 June 2012*, 5 January 2016, http://www.ae.utexas.edu/news/504-todd-humphreys-research-team-demonstrates-first-successful-uav-spoofing.
[73] Timothy L. Thomas, "Hezbollah, Israel, and Cyber PSYOP," *IO Sphere*, Joint Information Operations Warfare Center, San Antonio, TX. Winter 2007, 30; PSYOP is the acronym for Psychological Operation. Note: US joint doctrine has changed the name of the military capability PSYOP to Military Information Support Operations (MISO).
[74] Ibid.
[75] Information–related capability (IRC) is a term of art defined in US Joint doctrine as a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. US Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02, Washington DC: CJCS 8 November 2010, As Amended Through 15 November 2014, 121.
[76] Rogers, *Statement Before Senate Armed Services Committee*, 19 March 2015, 9.
[77] David Robb, *Sony Hack: A Timeline*, 19 December 2014, http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/; The entire printed collection of the Library of Congress can be stored on 10 terabytes of data.
[78] Small Wars involve a wide range of military operations in conflicts involving states or nontraditional actors, generally over a protracted timeline, characterized by a combination of physical violence and non-kinetic forms of influence requiring tightly integrated application of diplomatic, informational, economic, and military means. US Marine Corps. *Small Wars / 21st Century* (Marine Corps Combat Development Command: Quantico, VA, 2005), 3.
[79] Sun Tzu, *The Art of War,* trans. Samuel B. Griffith (New York: Oxford University Press, 1971), 130.
[80] Ibid.
[81] Corbett, *Some Principles of Maritime Strategy*. 95.
[82] Milan Vego, Lecture to Naval War College Joint Military Operations Department faculty January 9, 2012.
[83] US Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02, Washington DC: CJCS 8 November 2010, As Amended Through 15 June 2013, 70.
[84] General James E. Cartwright, USMC, Vice Chairman of the Joint Chiefs of Staff Memo, July 2010, Joint Terminology for Cyberspace Operations.
[85] The Internet of Things (IoT) has been defined in Recommendation ITU-T Y.2060 (06/2012) as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and

virtual) things based on existing and evolving interoperable information and communication technologies, 12 February 2016, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.
[86] Cyberspace systems are electronics that use computer software to run on code that moves through cyberspace. Cyber weapons may be any type of code or content that is able to make electronics act independent of the owner's intent or coerce human's to act.
[87] House of Representatives Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence; and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies and the Homeland Security Policy Institute at The George Washington University, *The Iranian Cyber Threat to the United States*, 1.
[88] Ibid, 4.
[89] Ibid.
[90] Cited in Timothy L. Thomas, *Dragon Bytes Chinese Information War Theory and Practice* (Fort Leavenworth KS: Foreign Military Studies Office 2004), 32.
[91] These concepts are adapted from Corbett's ideas on sea control.
[92] Anonymous is a hacktivist collective that pushes their ideology by attacking those with whom they disagree. Much like cyberspace, they are complex and adaptive. Their actions and objectives center on the use of cyber force nefariously to gain personal information in order to coerce or compel (blackmail) their targets into acting in desired ways. The ubiquity of cyberspace is used to protect their anonymity. They take advantage of crowd psychology, where ordinary people can gain direct power by acting as a collective. Anonymous have conducted operations against a variety of groups, including the Church of Scientology, one of Mexico's most powerful drug cartels, Los Zetas, various governments and their defense networks, numerous global corporations, banks, and individuals.
[93] Admiral Michael Rogers, USN, Commander, U. S. Cyber Command and Director, National Security Agency, *Testimony to House (Select) Intelligence Committee on Cybersecurity Threats: The Way Forward*, November 20th 2014.
[94] DHS Alert (IR-ALERT-H-16-056-01), *Cyber-Attack Against Ukrainian Critical Infrastructure*, *February 25, 2016*, 1 March 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.
[95] Tami Abdollah, Sophisticated *Attackers Hacked Ukrainian Electric Grid,* 1 March 2016, http://www.military.com/daily-news/2016/02/27/sophisticated-attackers-hacked-ukrainian-electric-grid.html#.VtMOZ9poMpw.mailto.
[96] DHS Alert (IR-ALERT-H-16-056-01), *Cyber-Attack Against Ukrainian Critical Infrastructure. February 25, 2016*.
[97] Abdollah, *Sophisticated Attackers Hacked Ukrainian Electric Grid.*
[98] Amanda Vicinanzo, *Russian Malware 'BlackEnergy' Infiltrates US Critical Infrastructure,* 11 December 2014, http://www.hstoday.us/channels/dhs/single-article-page/russian-malware-blackenergy-infiltrates-us-critical-infrastructure.html.
[99] Michael Joseph Gross, Silent *War*, 23 August 2013, http://www.vanityfair.com/culture/2013/07/new-cyberwar-victims-american-business
[100] Andro Barnovi, Deputy Defence Minister of Georgia, Brief to the "Cyber Defence and Network Security Conference" London, January 2012.
[101] David Hollis, "Cyber War Case Study: Georgia 2008." *Small Wars Journal*, 6 January 2011, 8.
[102] Cyber fires may be depicted as Operational Fires – defined as the application of one's lethal and/or nonlethal firepower for generating a decisive impact on the course and outcome of a campaign or major operation. They represent today an inherently multi-service or joint function. They are not simply fire support; hence, the success of an operational manoeuvre is not necessarily dependent on these fires. However, they can facilitate one's operational manoeuvre. They are conducted in the operational

and/or strategic depths of the enemy's defenses. Milan N. Vego. *Joint Operational Warfare Theory and Practice* (Newport RI: Naval War College, 2009), VIII-59-60.

[103] Rafal Rohozinski, CEO, The SecDev Group, Brief to the "Gaps in Thinking About Cybered Conflict and Governance Workshop" Brown University and US Naval War College, Providence, RI., June 7, 2013.

[104] Ryan Singel, *Egypt Shut Down Its Net With a Series of Phone Calls,* 12 December 2012, http://www.wired.com/threatlevel/2011/01/egypt-isp-shutdown/.

[105] Ibid.

[106] James Cowie, Renesys Blog, 12 December 2012, http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

[107] Scott-Railton's Voices Feeds were collaborative and trust-based, low-bandwidth conduit for the voices of Egyptian and Libyan people in conflict. For more information on John Scott-Railton, visit his web site, http://johnscottrailton.com/the-voices-feeds/. You may also view an interview Scott-Railton did at http://www.youtube.com/watch?v=wUw-MzjVltI.

[108] Ujjwal Singh and AbdelKarim Mardini, Google Blog, 12 December 2012, http://googleblog.blogspot.com/2011/01/some-weekend-work-that-will-hopefully.html#!/2011/01/some-weekend-work-that-will-hopefully.html.

[109] Paul Cornish, *The Vulnerabilities of Developed States to Economic Cyber Warfare*. Chatham House 2011, 11.

[110] Jordan Robertson and Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era*. Bloomberg News, 12 December 2014, http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html.

[111] A major part of Moscow's twenty–first century security strategy is built on the sale of oil and gas from its resource rich former satellite states to an energy dependent Europe. Moscow's ability to control or at least heavily influence the economies in the Caucuses and Central Asia is closely linked to its oil and gas trade.

[112] International Finance Corporation, Principal Economic Benefits of the BTC Project, 17 December 2014, http://ifcext.ifc.org/ifcext/spiwebsite1.nsf/0/e0bf99bac8cdd8e5852576c10080cbda/$FILE/attachment%202--%20Principal%20Economic%20Benefits.pdf.

[113] Robertson and Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era*.

[114] Ibid.

[115] Damien McElroy, *Georgia: Russia targets key oil pipeline with over 50 missiles*, 17 December 2014, http://www.telegraph.co.uk/news/worldnews/europe/georgia/2534767/Georgia-Russia-targets-key-oil-pipeline-with-over-50-missiles.html, and Georgian Ministry of Foreign Affairs, 18 December 2014, http://www.mfa.gov.ge/index.php?lang_id=ENG&sec_id=461&info_id=7484p.

[116] Robert M. Lee, Michael J. Assante, and Tim Conway, ICS CP/PE (Cyber-to-Physical or Process Effects) Case Study Paper – *Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack*. SANS Industrial Control Systems, December 2014.

[117] Ibid.

[118] Robert A. Miller and Daniel T. Kuehl, *Cyberspace and the "First Battle" in 21st-century War*, Center for Technology and National Security Policy National Defense University, Defense Horizons Number 68, September 2009.

[119] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House) February 1999, 188.

[120] Ibid., 199.

[121] Corbett, *Some Principles of Maritime Strategy*, 69.

[122] Clausewitz, *On War,* 358.
[123] Rogers, *Statement Before Senate Armed Services Committee*, 19 March 2015, 9-10.
[124] Chris C. Demchak, *Wars of Disruption and Resilience Cybered Conflict, Power, and National Security*. (Athens, GA: The University of Georgia Press, 2011), 72.
[125] Corbett, *Some Principles of Maritime Strategy*, 2-3.

The Corbett Centre for Maritime Policy Studies aims to promote the understanding and analysis of maritime history and policy and to provide a forum for the interaction of academics, policy-makers and practitioners.

The Corbett Centre for Maritime Policy Studies
Defence Studies Department
Joint Services Command and Staff College
Defence Academy of the United Kingdom,
Shrivenham, Swindon, SN6 8LA, United Kingdom

Email: corbettcentre.jscsc@defenceacademy.mod.uk

Copies of previous Corbett Papers are available from:
http://www.kcl.ac.uk/sspp/departments/dsd/research/researchgroups/corbett/publications/corbettpapers.aspx

The Defence Studies Department is part of the War Studies Group, King's College London.