lastline™

Asynchronous Warfare

The Strategies and Tactics That Give Attackers the Advantage in the Cyberwar That is Already Being Waged

Contents

"The greatest victory is that which requires no battle.
The supreme act of war is to subdue the enemy without fighting."
— Sun Tzu, *The Art of War*

Why are defenders always underprepared?

If someone did actually declare cyberwar, what would you do differently?

In this paper we attempt to answer both questions, to raise awareness, and to speed the adoption of advanced technology that can fight the cyberwar that's already being waged.

Asynchronous Warfare

We live in the age of the world order being challenged. The beginning of the 21st century will probably be looked back upon by future generations as a time of curious paradoxes: while our technical achievements appear to transform us into digital demigods, our ability to create reliable order out of chaos is not keeping pace, resulting in a world becoming unrulier every day. Or, as former CIA Director George Tenet once said: "We have built our future upon a capability we have not learned how to protect."[1]

We are constantly creating new ungoverned spaces of interaction while retreating from others where our methods of establishing order failed. This is one reason why the global balance of power is in a process of restructuring. Power migrates especially from the liberal West to any actor adaptive, smart and determined enough to prevail in this hypercompetitive "wild west" environment.

The Internet has created tremendous access to information, improved global interaction and engagement, and spawned new businesses and innovative business models. It has also completely changed what it means to be secure. And while security has always been seen as an important element that must be considered when moving anything online, security risks have escalated to a much higher level of importance—one that few truly appreciate or understand. The Internet is now a war zone, and the battle being waged is a skewed one, with the bad guys having the upper hand. But organizations have not adapted their security strategies accordingly.

In this paper we'll explore what this strategic imbalance looks like, and how the attackers are not just after a quick buck but a fundamental weakening of Western economies that tips the global economic balance of power in their favor, with every business of any size being caught in their cross hairs. We'll conclude with four Golden Rules that will help fend off this sustained attack.

More specifically, we will examine:

1. A time-proven strategy for a type of insurgent warfare that led to spectacular victories in conflicts such as the Vietnam War. Called "protracted people's war" by Mao Tse-tung, in this paper it will be named after its most relevant characteristic: *Asynchronous Warfare.*
2. Potential parallels between characteristic elements of asynchronous (ground) warfare in the past and the conflicts happening these days in the cyber domain.
3. The specific phases of asynchronous warfare strategy, and how the telltale signs of these strategies being applied in the cyber domain are already visible.
4. Strategies that organizations can adopt today to respond to the escalated level of threat presented by the online war we're now fighting.

Roots of Asynchronous Warfare

In order to understand what's happening today in the cyber realm, we first need to understand what asynchronous warfare is and how it operates in conventional warfare.

From the perspective of international relations, among the most important reason for the demise of the international order is the fact that the West has lost much of its aura of superiority in warfare since 9/11. Although conventional capabilities, at least regarding the United States, are still able to deter direct confrontation, the situation appears different when it comes to more unconventional forms of warfare. Here, the US and its allies have displayed shortfalls that did not go unnoticed by revisionist states like Iran and North Korea, and non-state actors such as ISIS and Al Qaeda, and encourage them to employ alternative strategies of political aggression.

That said, at the center of attention of this ominous development stand Russia and China. These great powers are proving especially adept at using a host of means to advance their power position in the world. For they have at their disposal a particularly successful alternative to violent political conflict[2], the basics of which were conceived by Vladimir Ilyich Lenin and his Bolshevik comrades-in-arms almost a century ago.[3]

It was eventually perfected by Asian communist leaders Mao Tse-tung (who called the concept "protracted people's war"[4]) in China and Ho Chi Minh in Vietnam. Proving to be radically effective, the Vietnamese under "Uncle Ho" and his general Vo Nguyen Giap employed the strategy[5] to win against France, the United States, and China in the course of less than 30 years. But how is it possible that these ill-equipped insurgency movements won, despite their glaring material inferiority? How could the world's leading military be forced to leave Vietnam without victory after almost two decades of intense engagement?

The answer lies in the application of a strategy that works by keeping the conventional forces off-balance at all times. A concept developed by military theorist John Boyd helps to understand how this can be accomplished. The former aviator used his experiences in air combat to scrutinize on the mental process that precedes action.

The concept he came up with he called the OODA-Loop.

It has four steps:

observe
orient
decide
act

While all steps are important, it is the second, the orientation step, that merits special attention. If an insurgent (in this case) is so flexible that he can adapt to any action of a conventional force quicker than they do, he is able to "break into" the OODA-Loop of the conventional army before it had time to orient itself.

Imagine you find yourself in a boxing match with someone three or four times quicker than you are. Every time you observe where he is and take aim to punch him, he is somewhere else already. This leads to you punch thin air, an ineffective and tiresome method of fighting, made even worse by the fact that your quicker opponent has plenty of time to search for openings in your defenses—and counterstrike.

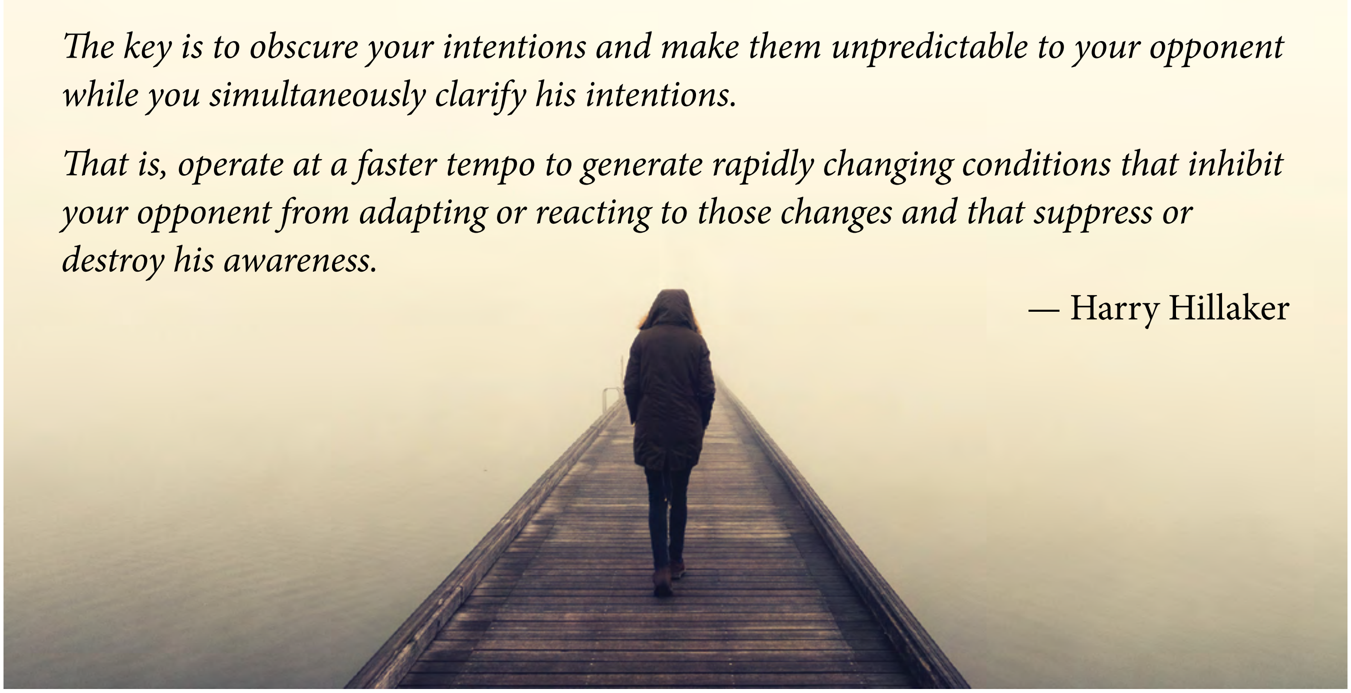
From a systemic point of view, one could say that if a strategy succeeds in constantly breaking into the defender's OODA-Loop, it keeps him from synchronizing his actions with those of the attacker. He will always be too late and mispositioned. Focusing on the mechanisms that make this method successful, therefore, it is aptly named Asynchronous Warfare.

The term asynchronous had been used in the first decade of the new millennium[6] but appears to have lost in academic usage against the term "asymmetric" warfare. This is unfortunate, given that asynchronous in the sense of "out of step" fits perfectly with the idea of breaking into an enemy's OODA-Loop and has high descriptive value for what happens in a conflict between conventional and unconventional actors.

One reason is that the level of awareness and the recognition of the start of a conflict between attacker and defender is almost always asynchronous. If a defender does not recognize early attacks, or at least does not recognize them for what they are, he has not even braced himself for an increase of offensives when the attacker is already well into the execution of his strategy.

This situation can be especially relevant in cyberspace, where the impact of an attack is often not known until much later. By necessity, the technical and operational response of the defender to attacks is also asynchronous, for as soon as he realizes he is in a longer-term conflict, he finds himself in a position of constant defense, whereas the offensive attacker can dictate the pace of operations.

Asynchronous Warfare Strategy and Phases



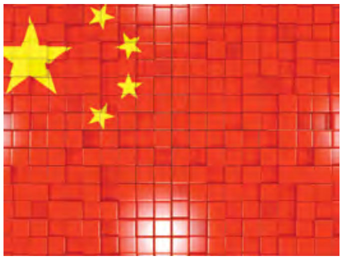
> *The key is to obscure your intentions and make them unpredictable to your opponent while you simultaneously clarify his intentions.*
>
> *That is, operate at a faster tempo to generate rapidly changing conditions that inhibit your opponent from adapting or reacting to those changes and that suppress or destroy his awareness.*
>
> — Harry Hillaker

A well-executed asynchronous warfare strategy, as applied to conventional warfare, breaks into the enemy's OODA-Loop on all four levels of military theory: tactical, operational, strategic, and grand strategic.

Tactical: Through a system of decentralized (localized) command and control, the insurgents are regularly better informed and much more flexible than the conventional defenders with their cumbersome hierarchical organization and can choose time and place of encounters. This, in theory, can also work in reverse, where the defenders are the ones applying asynchronous strategy and it's the attackers who rely on conventional methods.

Operational: For the same reason, the insurgents easily avoid large troop concentrations. Preparations for big unit operations never go unnoticed, involve many people potentially leaking information and their intentions are usually easy to grasp. While the conventional actor therefore tries to orient himself regarding the positions where insurgents are to be expected, they have usually already changed positions.

Strategic: Asynchronous warfare replaces the conventional focus on active destruction through concentrated firepower with a permanent attrition of the enemy. It shifts the key segment of war from the (often idealized idea) of a decisive battle to a much longer phase of constant disintegration, to "death by a thousand cuts."



This, however, means that the corpus of causal mechanisms in military theory has to be transformed from a principle of effectiveness (greater firepower) to one that pays premium attention to efficiency (relatively better cost-benefit ratio).[7] This mosaic approach to conflict in the cyber sphere prompted the NSA deputy director George Barnes to recently state that rather than one, devastating cyberattack, there has been a "slow drip" of "continual theft of intellectual property from our industries."[8]

Grand strategic: The major challenge from the perspective of Western grand strategic thought when facing an asynchronous warfare strategy lies in the adaptation of the concept of threat. Because from a Western perspective, war (and therefore a perception of existential threat) really only begins with large-scale physical destruction and—especially important in liberal political thought—with people dying in unusually large numbers. Liberalism tends to pigeonhole other, lesser forms of political aggression into the rubric of criminal offenses. This, however, is a recipe for disaster in an asynchronous conflict whose general aim it is to avoid large scale operations and instead destroy the function of the political system[9] while operating "below the threshold level of war."[10] The decisive phases of a protracted or asynchronous war, in other words, often take place long before Western analysts would recognize an existential threat.

Instead of measuring threats in terms of potential deaths, therefore, the more reasonable way to measure them would be the degree to which systemic function is impeded—that is, whether an attacked system is still able to function properly. Given that the orderly function of our societal systems and subsystems is the core requirement for the stability of our complex societies, the collapse of these systems can lead to chaotic circumstances (and then potentially to the death of many).

A Three-Phased Strategy

Any stable geopolitical state is based on trust between the government and the citizens on whose resources and compliance the state depends. In a nutshell, asynchronous warfare strategy is structured in three phases, all of which combine physical and perceptional means to destroy this trust. Each phase exploits specific vulnerabilities of the attacked and thereby prepares the "battlefield" for the next phase long before it actually materializes. Each phase also is a fallback position in case the actions on a certain level are unsuccessful.

We start by describing each phase as it works in a physical war where the goal is to take control of a geographic area. Later we will see how this strategy and these three phases work in cyber warfare.

First Phase: Subversion of Political Trust

In the first phase, the aim is to identify disaffected groups that oftentimes can be found on the political fringes of society.[11] The actual political positions of these groups are mostly unimportant, relevant is only their potential for mobilization against the current order. Agitation specialists are sent to these groups, whose purpose is to further mentally separate their members from the state.[12] If the agitation proves successful, these groups are used to establish cells of a nascent covert insurgent infrastructure[13], providing in-country intelligence, personnel, and material resources for the attacking side.

Once the infrastructure is sufficiently settled, the first public actions are planned and executed. Their aim is to spread doubts about the government in an increasingly larger share of the population. For that end, political discord—which can be found lying dormant in any society—is fostered and intensified by occupying topics of general interest. The main interest is to depict the government as unjust and illegitimate.

The next step is to identify persons and institutions that symbolize the power of the attacked political entity. Preferred targets are politicians and members of the security apparatus and their respective agencies. By harming them, the attackers demonstrate to the public that the authorities are incapable of protecting even these beacons of their government.

Second Phase: Bleeding The Enemy White

In the wake of the first successful operations, the ranks of the insurgents swell and even more operations can be executed. In due course, the attacker starts a plethora of violent incidents. They metastasize like a cancer in the territory of the defender who usually is quickly overwhelmed by the requirement to secure so many objects and areas at the same time. Attack operations are carefully planned to make sure that the attacked are outnumbered and that reinforcements for the defenders arrive only after the fight is over. Again, timing is a crucial element: if the defender would be able to prepare for the attack, the lightly equipped attackers would not stand a chance.

Since the defender cannot position troops everywhere at the same time, sooner or later he finds himself in a real dilemma: if he tries to defend against all possible attacks, his forces are overstretched and he can defend nothing effectively. If he abstains from defending his symbols of power, in contrast, he highlights his helplessness and loses the trust and compliance of its citizens (or stakeholders) in its capability to protect them. As a consequence, a defender usually concentrates his forces in the more relevant areas of his territory, especially the capital, thereby exposing less critical areas of his territory to the enemy, which quickly begins to fill the void and establish overt control of the area. The attacker now can start to set up more conventional forces with better training and equipment that carry a heavier punch.

For the defender, a vicious cycle starts: ever heavier equipped formations of the attacker can take hold of increasingly more symbolic assets, forcing the defender to further concentrate his forces around his symbolic core. As a consequence, the attacker can seize increasingly bigger parts of the defended territory. He can also start to mount more intensive attacks to actively deplete the ranks of security forces and to shatter their morale. Sooner or later, the resources of the defender begin to dwindle, as does the trust of the population in his eventual victory. Citizens will start to wonder if it would not be wise to come to an arrangement with the attacker—the defender loses his political power and thereby access to the resources of the population.

Third Phase: Coup De Grace

The main—as a matter of fact, the only—application of large-scale conventional warfare is in phase III when the attacker is completing the takeover of the country or territory being attacked. However, in a protracted war the third phase only begins when the attrition of the defender is already so profound that he does not stand a real chance of winning anymore. The conventional fighting is only intended to wear down the remnants of his armed forces and to finish the war as quickly as possible.

Asynchronous Warfare 2.0

The cyber realm has attracted a variety of revisionist actors who do not have the means to win in a conventional conflict against the West, but who do have a good understanding of the possibilities afforded by the Internet.

Instead of measuring threats in terms of potential deaths, as is done with conventional warfare, the more reasonable way to measure them would be the degree to which systemic function is impeded—that is, whether an attacked system is still able to function properly. Given that the orderly function of our societal systems and subsystems is the core requirement for the stability of our complex societies, the collapse of these systems can lead to chaotic circumstances (and then potentially to the death of many). Therein lies the objective of the attackers in today's asynchronous war.

The cyber realm as a battle space is attractive for several reasons:

1. Cyber operations offer compelling cost-benefit-ratios for attackers who do not have sufficient conventional means to win an all-out (conventional) war, but who do have many bright young IT minds.[14]
2. Personal assets do not have to be physically infiltrated into another country to develop a covert infrastructure or occupy sensitive positions in the attacked society.
3. Attackers can operate in ambiguity, which oftentimes makes attribution difficult, if not impossible.[15]
4. Finally, given that every advanced system, military and civilian, will in the future be operated autonomously, there is no denying that an enemy's control over IT operations will become even more critical than it already is today.

The Target is the Economy, Which Depends on Technology

In military parlance, a vulnerability that, when properly exploited, decides a conflict is called a **Center of Gravity**. With the ever further increasing interoperability of every military unit, from a tank battalion to a carrier strike group and upwards, becoming a reality, IT-based command and control systems are perhaps the closest incarnation of a perfect Center of Gravity that ever existed. Given the world's (and especially the West's) rapidly increasing dependence on IT for its organizations to function, cyber operations move from the fringes to the very center of future warfare.

This development is obviously not limited to the military but takes place in all other sectors of society as well, especially the economy. From critical infrastructure, supporting our fragile urban existence with water and electricity, to the captains of industry producing the wealth necessary to keep things running, all elements of an economy depend on the uninterrupted operation of IT systems. This would, in and of itself, be problematic enough if we still lived in an age in which hacking is "only" related to criminal intention. It is a fact, however, that when it comes to organized cybercrime there is no longer a strict separation between organs of the state and the criminal civilian elements, and that a core element of Western liberal order must be considered weakened today by the efforts of a wide variety of combatants—whether civilian or military—in these undeclared wars.

The appeal and resulting impact of cyberconflict are not hard to see:

1. Successful attacks against companies damage the reputation of the government as a capable defender of society.
2. Attacks weaken the attacked state by stealing innovative knowledge.
3. Attacks carry a low risk of (potentially military) escalation if uncovered.

Since the development of technology in the West is the job of civilian companies, critical knowledge in the defense, software, finance, pharmaceutical, or biotech industries, to name but a few, could be stolen or—even worse—corrupted by foreign invaders.[16] In addition, the economic damage caused by cyberattacks impact countries by pushing them towards economic recession and depression. Economic downturns in individual nations could encourage an internal focus on politics and facilitate an environment of a political isolationism agenda and an abandoning of foreign policy commitments. Every cyberattack that causes economic damage is potentially another nail in the coffin of existing international treaties and relations and yet another victory for a divide and conquer strategy.

Three Phases—Redux

Earlier we described the three phases of an asynchronous warfare strategy as applied to conventional warfare. We now explore how these same three phases apply to cyber warfare.

Phase I: Social Media Subversion and Digital Insurgent Infrastructure

(Dis-)Information Operations: If a country engages in an asynchronous war against a much stronger adversary today, it would begin with Information Warfare[17] operations in the cyber realm.[18] This allows the attacker to prepare the battlefield long in advance. By meddling with the U.S. presidential election, for instance, the Russian troll armies tried to *"undermine public faith in the US democratic process"*[19] and on a more general level "*to undermine the US-led liberal democratic order.*"[20]

The idea behind these measures, which in quite similar form also took place on numerous other occasions throughout Europe, is to create a double effect: not only could a certain limited effect on election results be achieved, but the interference with elections also signaled clearly to the respective populations that someone was "inside" the election process. For liberal societies that draw their legitimacy to a large extent from the trust the citizens have in due process, this poses a great danger. *"Russian disinformation does not aim to provide answers, but to provoke doubt, disagreement and, ultimately, paralysis."* [21] With criminals using new technological capabilities such as Artificial Intelligence and machine learning, the fight to discern the truth from fake is becoming increasingly difficult.[22]

It is not surprising that the battlefields for information warfare today are social media networks. Because social media puts an end to journalism's monopoly on information dissemination, the direct access to millions of citizens provides attackers unparalleled opportunities for undermining order and creating social discord.[23] Today, any type of news—real or fake—can reach social media users more or less unfiltered. Given that humans are strongly influenced by their primordial instincts, the oftentimes flavorful pieces of uncontextualized raw information tilt the balance between rational thought and emotion markedly to the latter. Social media is the perfect arena for the great simplifiers and those intent on undermining the truth and trust.

“Better” yet, public opinion can also be influenced with relatively frugal means. A person working as disinformation mercenary in a “troll farm” or directly for government agencies is oftentimes supported by a considerable number of automated social media accounts (“bots”), affording a single person tremendous impact. The bot’s job is to trick the algorithms of social networks into believing that the troll’s post receives a lot of support by other users, create a weight of opinion that make it look like there is huge support for an argument, while in fact it is artificially created.[24] With the combination of a number of trolls proficient in the respective foreign language and a supporting army of social media bots, much damage can be done by little means.

Infiltration: While these are the more or less overt operations in phase one, another operation, equally important at least, is taking place in much greater secrecy. Whereas in former times insurgent infrastructures were created through the dangerous business of approaching persons and convincing them to become members of a cell, it is the infiltration of cyber assets into Western IT systems in all spheres of society that creates the basis for the second phase of attack.[25]

According to experts, countries such as Russia, China, North Korea, and Iran have been mapping IT systems of the U.S. industry for years.[26] Then-Director of National Intelligence James Clapper reported in 2015:

> *“…Russian cyber actors are developing means to access industrial control systems (ICS) remotely. These systems manage critical infrastructures such as electric power grids, urban mass-transit systems, air traffic control, and oil and gas distribution networks. These unspecified Russian actors have successfully compromised the product supply chains of three ICS vendors so that customers download exploitative malware directly from the vendors’ websites along with routine software updates, according to private sector cybersecurity experts.”* [27]

In July 2018, Homeland Security Officials reported that Russian military hackers were targeting the American electric utility grid, where they attempted to plant malware.[28]

The covert mapping of IT systems provides attackers an excellent understanding of their strengths and weaknesses. This allows them to launch effective attacks and/or take them over and use them for their own purposes in the future. Speaking metaphorically, through mapping, attackers learn on what pillars the entire system rests and how it functions—in order to plant explosives in the right places.

In fact, the truth is very close to this metaphor. Intelligence agencies in Western countries are increasingly vocal about the danger of foreign cyber operators capable of bringing down entire IT systems. In April 2018, U.S. and British intelligence services published a joint statement in which they warned of a global campaign against millions of machines used to direct data traffic in the Internet. Targets again were of functional and symbolic importance, including critical infrastructure[29] and communications providers, government departments, and large corporations.[30] Director of U.S. National Intelligence Dan Coats stated in July 2018 that “the digital infrastructure that serves this country is literally under attack.”[31]

Phase II: Conflict in the Cyber “Gray Zone”

In the logic of asynchronous warfare, the second phase begins when sufficient doubts about the cyber defensive capabilities of the government and security apparatus have been planted in the minds of a segment of a targeted population and when the “insurgent” infrastructure is sufficiently established. These conflicts take place in what was recently described as a “gray zone.” [32] One of the characteristics of a gray zone is that actions can by intent and motivation be linked to certain actors, while it is impossible to prove their perpetration with a degree of certainty that would convince a court—or even public opinion—of the perpetrator's guilt.

Strategically, this creates an atmosphere of diffuse uncertainty, in which it becomes difficult for the attacked to reassure their citizens and allies that they are actually in charge of what happens.[33] Notably, in Phase II the attackers use chaos and disorder as a weapon to undermine governments. That said, they are not interested in creating a situation that is completely uncontrollable for all times. Although adept at navigating markedly more disorderly waters than the West generally is, the aspired end-goal is a situation that can be controlled, either through proxies from a distance or directly through conventional structures of authoritarian rule.

In terms of asynchronous warfare theory, the attackers are in the phase of violent subversion in which they attack highly symbolic assets of the defender and plant a covert infrastructure. Through highly symbolic actions they signal to the attacked population that they could wreak havoc if they chose to and that their defenders in contrast are helpless guardians. But what are highly symbolic targets? A matrix of symbolic value could be constructed along the lines of the factors of quality and quantity.

From a qualitative point of view, the greater the nimbus of power that goes along with an organization, the greater the symbolic success if it can be hacked. From the standpoint of symbolic communication, embarrassing the CIA, FBI, or Special Operations Command, for example, is worth much more than hacking the Department of Veterans Affairs or Agriculture. Given the highly symbolic position the economy has, especially in liberal societies, corporations are prime targets as well. Although few citizens are usually interested in how their security is organized, most would recognize it as a symbolic defeat if a corporation such as Apple, Microsoft, or IBM would be operationally disabled through a hacking attack.

The quantitative dimension refers to the number of people affected. A classical example is the public transportation infrastructure. Although not really severe in terms of ultimate consequences, a break down of the New York City Subway for even a short time will affect a lot of people.

The cyber age brings a new dimension to this matrix, however. Through scalability, successful attacks on one device can have cross-sectional effects. There is software that is so basic and used in so many cases that it could lead to major problems if successfully attacked. Examples include pacemakers[34], insulin pumps, and other such devices that probably keep millions of people in the Western world alive and well. Another is Microsoft Windows, on whose function the vast majority of computer operations depend. Never before was it theoretically possible to affect so many individuals and entities with so little means.

A very basic threat matrix of symbolic impact can easily be made for a great variety of topics, in this case for the health care sector.

Symbolic Value	Low Qualitative Value	High Qualitative Value
Low Quantitative Value	Impeding the delivery of non-critical medication in one case	Postponing a time-critical operation
High Quantitative Value	Impeding the delivery of non-critical medication in an entire region	Postponing all time-critical operations

The operational aim of the attacks is to encourage the defender to concentrate his scarce IT security resources around his most important assets. The attacker's hope is that the defender thereby exposes or neglects his

IT periphery, which makes it possible to incrementally increase control over ever-larger segments of an IT system. This principle, notably, is equally applicable for a single corporation network or an entire country.

In order to support this retrenchment movement, spectacular attacks on high-value targets will from time to time occur, but mostly for symbolic reasons. One especially thorny problem connected to different levels of security at the center and the periphery is supply chain security.[35] National or international subcontractors who are not properly secured are easy prey for attacks while at the same time providing oftentimes easy access to the client company.[36]

Pushing for cyber due diligence to make sure that subcontractors (and their subcontractors and so forth) are compliant with cybersecurity regulations is therefore a tremendously important aspect of defense. Given the expenses this implies, large corporations are well advised to price in the costs for cybersecurity throughout their entire supply chain.

On a tactical level, Phase II operations in the cyber realm also share some of the basic characteristics with their analogue siblings, especially with regard to the factors of time and place. Time is on the attacker's side in two senses: not only could an attacker decide to start an ongoing attack at any time, but, more importantly, he can position his software long in advance in the IT system and decide when to activate it. Choosing the place could in the cyber context mean choosing an attack vector: not only can an attacker decide what part of the IT system to attack, but he can attack parts that are not immediately critical but might be useful in a bigger context. He could for example hope for cascading effects that may indirectly bring down much bigger targets than the one he actually hacked.

There is one marked difference to earlier times, however: Today's cyber attackers have an important advantage over their earlier precursors insofar as their "gray zone" fighting can be conducted mostly in the dark, whereas fighting for local control was inevitably a public affair.

There are also similarities. In both cases the attacker strives to eventually reach a position of control over a country—either physical control or economic gain by weakening the economy of the attacked—compelling the defender to do what he, the attacker, wishes. Only that today this includes the ability to control or harm the defender's IT systems.

As soon as a sufficient degree of control over IT systems is established, the (often quite extended) process of tilting the balance of forces is the next main priority. This includes control of an increasing number of IT systems, sophistication of attack and defense methods, and financial and intellectual property assets. This is the state of conflict the West is probably currently in with regard to Russia and China.

While cyberattacks are simply a given in this day and age, at least for the time being spectacular offensives with the aim to destroy or permanently disable a system are at least not overly common in the West. That said, there are international cases that demonstrate fairly well the approach as well as the intentions expected to be seen in Phase II operations. An especially descriptive example is the operations Russia conducted in Ukraine in 2015 (see sidebar on pages 14-15). More recently, a potential Russian-Iranian cooperation managed to damage thousands of computers at the world's largest corporation, Saudi Aramco, with malware named Triton.[37] There's suspicion that the hackers were attempting to start an explosion at a petrochemical plant jointly owned by Saudi Aramco and Dow Chemical by compromising controllers (thought to be secure) intended to regulate critical factors such as voltage, pressure, and temperatures.[38]

Phase III: Overt Fighting—Really?

In asynchronous warfare 1.0 the third strategic phase is devoted to conventional battles to eradicate the defender's last organized resistance. For the time being, this will also be valid for the end of an asynchronous warfare 2.0.

That said, there is at least the theoretical possibility that the struggle ends differently in the 2.0 variant. Spinning the idea of the IT systems as Centers of Gravity further, the question is whether it would not be enough to control the systems that control the weapons. Corrupting, for example, command and control systems of the U.S. military to a degree where no commander could be sure that the information he receives are genuine would create a situation in which fighting becomes pointless. Although this is a dystopian view of the future, it is not entirely unrealistic either.

Let's look at another scenario: if an attacker were indeed able to control computers running with Microsoft Windows, and could switch his control off and on like the Russians did with their control over the Ukrainian power plants, how long would it take for the West to consider a truce with the attackers? You will now probably be tempted to say that this is impossible or at least highly unlikely. And you would perhaps be right. But since we have such a hard time detecting ongoing long-term attacks, can we be sure about it?

OODA-Loop 2.0

Looking at the cyber challenges the IT security professionals are faced with today reveals remarkable resemblances when it comes to the four levels of strategic theory. Again, a defender is confronted with actions that directly aim to break into his OODA-Loop.

Tactical: The attackers can choose time and place of an attack. When the Computer Emergency Response Team (CERT) arrives, the attack has already occurred. Vice versa, counter attacks are problematic, because attribution is oftentimes hardly possible or even impossible. If it is impossible to identify an opponent,

2014 Ukraine

Ukraine is perceived by the Kremlin as Russia's backyard and as an important buffer state against NATO. When the Ukrainian government started to move its country in Western direction, therefore, the Putin administration reacted extremely determined.

Besides the well-known employment of the "little green men" occupation troops on Crimea and the ongoing support of "rebels" in Eastern Ukraine, *"Russian hackers have utilized spear phishing, malware, DDoS attacks, telephone denial of service (TDoS) attacks, and other forms of cyber disruption and espionage to conduct a steady drumbeat of cyberattacks targeting Ukraine's government, military, telecommunications, and private-sector information technology infrastructure."* [1]

The Russian cyber actions in Ukraine were planned long in advance and started under the codename operation Armageddon in mid-2013.[1] According to some sources, a particularly sophisticated attack took place in December 2015, when Russia hacked three distribution centers of a Ukrainian power provider, shutting down the energy for more than 220,000[1] citizens in a region were heating is dependent on electricity.[1]

According to one source, the hackers might have used the cyber surveillance software BlackEnergy to map the IT system prior to the attack.[1] The degree of sophistication of this and another malware named Ouroboros, which also was found to be used for command & control of malware via satellite, makes it very likely that its operators are linked to the Russian government.[1] Investigations by the U.S. DHS revealed that the legitimate credentials of power grid operators had been "harvested" by unknown means, most likely through spear-phishing. A regularly used method by Russian hackers to obtain access to IT systems, spear phishing highlights the impact of human error in any system with human operators directly in the loop.

Human operators are a major weakness in all IT systems, often becoming victims of spear phishing attempts and thereby open the attackers a way however, it is equally impossible to bring the fight to him. Therefore, defense is the only, if deficient, strategy.

Operational: The sheer number of attacks in different places can easily overwhelm the incident responders. While this was already the case in asynchronous warfare 1.0, with a constant lack of security personal, it is much worse in cyber space. Because there are markedly fewer cybersecurity operators than security forces while at the same time the possibility to attack are more numerous yet.

Strategic: The West once more appears to be disoriented in the face of his constant positioning in the defensive. Faced with the challenge to secure his networks, he is once more caught in an arms race whose existence he has not completely realized yet. This time, however, as long as he does not adopt a doctrine that includes retaliation, he needs to develop purely defensive strategies—an ardent task, for purely defensive strategies have seldom been successful in history.

into the system. A small but, from an individual perspective, particularly unsettling part of these more or less hidden attempts of phishing are so-called "kompromat" operations, designed to gather compromising material about a person that can then be used for blackmail. Certainly not new in concept, the cyber realm provides kompromat missions an entirely new "hunting ground."

Not only is it comparatively easy to obtain badly secured personal information about almost anyone, but the cyber realm with its appearance of anonymity is ideally suited to create opportunities for misconduct. According to one source, Russia might be planning to apply these techniques on a massive scale by using machine intelligence, making it perhaps possible to blackmail a large number of unsuspecting persons.[1]

[1] *Information Warfare Handbook*, Keir Giles, p. 71.

Grand strategic: In the mindset of organizations in the Western world, the focus usually lies on optimal function in a "normal" situation, which is perceived as one of peace and order. Security, in contrast, is not among the core aspects of organizational architecture. This leads to insufficient resources invested in developing robust and resilient organizations. The grand strategy is continual attack that erodes both economic power through the simple, endless attrition of money and IP, as well as trust in the ability of government to secure its people, processes, and technology. Being under constant attack without realizing it leads to operations in perpetual crisis mode, to which Western organizations are unaccustomed and in which they are not as effective as they could be.

Four Golden Rules for Captains of Industry

The ever-increasing pace and scope of digitization is inevitable to keep our Western economies competitive. Without it, we will be outperformed in a heartbeat by economies leapfrogging stages of technical and organizational development.

However, if we continue with the digital revolution and increasingly use digital systems for organizing our life, our work, our production sites, and our defense, we will create a massive center of gravity in our IT systems. They are the hubs of societal coordination; they are the command & control systems of the 21st century. They will therefore increasingly be under attack.

Looking from an economic standpoint on the potential consequences of asynchronous warfare for the long-term productivity and prosperity of economies, it is probably fair to say that a further descent into Phase II gray zone conflicts cannot be in the interest of most. Western societies that rely on a stable, orderly, and secure economic and political environment are heading towards more uncertainty in their long-term interests. To address this, the following four "golden rules" might serve as food for thought.

1) Wake Up to the Situation

It is necessary to accept the fact that the economy has become a de-facto combatant in the ongoing conflict, and the conflict is on a global cyberwarfare scale. Corporations are used as pawns in the game to damage the population's trust in the ability of the government to uphold order and guarantee societal function. Therefore, expenses for IT security in corporations are directly beneficial to the protection of your assets.

2) It's All Just a Little Bit of History Repeating Itself

The Cold War was eventually won by a more or less stable societal consensus to infuse a substantial percentage of GDP into the development of new weapons systems at a pace the Soviet Union could not keep up with. This current conflict will also eventually be won by the side capable of introducing more sophisticated cybersecurity technology at a quicker pace.

3) Raise the Bar for Best Practices and Regulation

IT security is costly, it is complicated, and it demands continuous action. These are just three reasons why even large corporations can be inclined to bypass the topic now and then. The situation is even worse when it comes to the supply chain, oftentimes spanning dozens of typically smaller companies on several continents. As leaders, however, you have a great interest that your organization is secure and that the corporations comply with the highest standards of IT security. It is therefore on you to demand (and price-in) systematic efforts to keep up to date. Correct security is appropriate to the risk, put risk in the context of being a target of asynchronous cyberwar.

4) Push For Ever More Sophisticated Defenses

Improving the sophistication and capabilities of IT systems and security capabilities is the best shot at getting ahead of the cyber warfare problem. Sophisticated defenses will eventually deny success to the rather large community of single hackers and non-state groups with limited resources, which is a great deterrence. If someone repeatedly fails in hacking a system, he will eventually stop trying. This, in addition, will reduce the number of potential attackers markedly and make attribution easier. The more sophisticated the attack, the more likely it will also be to find identifying patterns. As soon as attacks can be attributed with a relatively high degree of certainty, credible retaliation regimes can be established. Therefore, make it a principle to constantly push for better and more sophisticated solutions. Constantly raising the bar of security and IT sophistication eventually can drain the swamp.

Endnotes

1. https://www.washingtonpost.com/investigations/understanding-cyberspace-is-key-to-defending-againstdigital-attacks/2013/06/03/d46860f8-ad58-11e4-9c91-e9d2f9fde644_story.html?utm_term=.48f27804de29

2. Media Ajir and Bethany Vailliant: Russian Information Warfare: Implications for Deterrence Theory, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Ajir.pdf

3. Thomas G Mahnken, Ross Babbage, Toshi Yoshihara: Countering Comprehensive Coercion—Competitive Strategies Against Authoritarian Political Warfare, Center for Strategic and Budgetary Assessments, 30 May 2018, p.11, https://csbaonline.org/research/publications/countering-comprehensive-coercion-competitive-strategies-against-authoritar/publication; Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, Katya Migacheva: *"Modern Political Warfare—Current Practices and Possible Responses,"* RAND Corporation, 2018, pp. 51-2, https://www.rand.org/pubs/research_reports/RR1772.html

4. http://www.marx2mao.com/Mao/PW38.html#s1

5. Douglas Pike, Viet Cong: Organization and Technique of the National Liberation Front of South Vietnam, (The MIT Press: new ed. 1970) pp. 37–146.

6. For example, the term was used by Thomas P.M. Barnett in a comment to Frank Hoffman's post "Are We Ready for Hybrid Wars?" 18 February 2008, http://thomaspmbarnett.com/globlogization/2008/2/18/warfare-now-is-both-asymmetrical-and-asynchronous.html

7. Oral evidence: Russia: Implications for UK Defence and Security, HC 763, House of Commons Defence Committee, 1 March 2016, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/oral/29915.html; https://www.cyberscoop.com/george-barnes-nsa-us-china-ip-theft/

8. https://brica.de/alerts/alert/public/1228100/nsa-official-foreign-hackers-have-pummeled-us-by-stealing-ip/

9. Barno, David and Bensahel, Nora: Fighting and Winning in the "Grey Zone", War On The Rocks, 19 May 2015, https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/

10. https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html; Charles Baudelaire, "The Generous Gambler"

11. Rick Noack: *The European Parties accused of being influenced by Russia*, The Washington Post, 17 November 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/11/17/the-european-parties-accused-of-being-influenced-by-russia/?utm_term=.74f1393f3abd; Alina Polyakova, Markos Kounalakis, Antonis Klapsis, Luigi Sergio Germani, Jacopo Iacoboni, Francisco de Borja Lasheras, and Nicolás de Pedro: *The Kremlin's Trojan Horses*, Atlantic Council Eurasia Center, November 2017, http://www.atlanticcouncil.org/images/The_Kremlins_Trojan_Horses_2_web_1115.pdf?ref=drnweb.repubblica.scroll-1; https://www.theatlantic.com/international/archive/2017/01/putin-trump-le-pen-hungary-france-populist-bannon/512303/; Ronald Brownstein: *Putin and the Populists*, The Atlantic, 6 January 2017, https://www.theatlantic.com/international/archive/2017/01/putin-trump-le-pen-hungary-france-populist-bannon/512303/

12. According to the glossary of information security terms of the Russian General Staff Military Academy, agitation is understood as influencing people or groups of people on an emotional level with the aim of prompting them to conduct specific actions. Dictionary of terms and definitions in the field of information security, Russian General Staff Military Academy, 2nd Edition, Moscow Voyeninform, 2008, p. 6.

13. Jeffrey V. Dickey; Thomas B. Everett; Zane M. Galvach; Matthew J. Mesko; Anton V. Soltis: Russian political warfare: origin, evolution, and application, Naval Postgraduate School, Monterey, June 2015, p. 24-5, https://calhoun.nps.edu/bitstream/handle/10945/45838/15Jun_Dickey_Everett_Galvach_Mesko_Soltis.pdf?sequence=1&isAllowed=y

14. Michael Connell and Sarah Vogler: *"Russia's Approach to Cyber Warfare,"* CNA Occasional Paper series, March 2017, p. 10, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

15. Alina Polyakova and Spencer P. Boyer: The Future of Political Warfare: Russia, The West, And The Coming Age of Global Digital

Competition, Brookings—Robert Bosch Foundation Transatlantic Initiative, March 2018, p. 2, https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf

16. A noteworthy point in case is the misappropriation of blueprints for the U.S. F-35 Joint Strike Fighter which ended up in the development of the Chinese J-31, affording the Middle Kingdom a technological tiger leap. https://www.reuters.com/article/usa-fighter-hacking/theft-of-f-35-design-data-is-helping-u-s-adversaries-pentagon-idUSL2N0EV0T320130619

17. http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

18. https://cepa.ecms.pl/files/?id_plik=2715

19. https://www.intelligence.senate.gov/hearings/open-hearing-intelligence-communitys-assessment-russian-activities-and-intentions-2016-us#

20. https://www.dni.gov/files/documents/ICA_2017_01.pdf

21. https://www.stratcomcoe.org/elucas-bnimmo-cepa-infowar-paper-no1-information-warfare-what-it-and-how-win-it

22. Alina Polyakova and Spencer P. Boyer: The Future of Political Warfare: Russia, The West, And The Coming Age of Global Digital Competition, Brookings—Robert Bosch Foundation Transatlantic Initiative, March 2018, https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf

23. For example, Russian trolls used pro- as well as contra- vaccine statements to enrage parents on either side. https://www.nytimes.com/2018/08/23/health/russian-trolls-vaccines.html

24. https://www.nytimes.com/video/us/politics/100000005414346/how-russian-bots-and-trolls-invade-our-lives-and-elections.html

25. See Keir Giles: Handbook of Russian Information Warfare, Research Division, NATO Defense College, November 2016, p. 11.

26. https://theconversation.com/with-hacking-of-us-utilities-russia-could-move-from-cyberespionage-toward-cyberwar-100503

27. James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, February 26, 2015, http://fas.org/irp/congress/2015_hr/022615clapper.pdf, p. 2-3.

28. https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html

29. In August 2018, IBM's cyber research division named X-Force Red has published information that the team has identified a number of critical vulnerabilities in emergency systems of major city infrastructures. So-called "panick hacks" in the worst case could lead to catastrophic events. https://www.bbc.co.uk/news/technology-45128053

30. https://www.bbc.co.uk/news/technology-43788338

31. Transcript of a speech delivered at the Hudson Institute on 13 July 2018. https://www.npr.org/2018/07/18/630164914/transcript-dan-coats-warns-of-continuing-russian-cyberattacks

32. Statement of General Joseph L. Votel, Commander U.S. Special Operations Command before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, 18 March 2015, p.7 https://docs.house.gov/meetings/AS/AS26/20150318/103157/HMTG-114-AS26-Wstate-VotelUSAJ-20150318.pdf

33. See Keir Giles: *Handbook of Russian Information Warfare*, Research Division, Nato Defense College, November 2016, p. 16.

34. https://www.zdnet.com/article/misfortune-cookie-vulnerability-impacts-medical-devices/

About the Authors

Dr. Bjoern Dennis Prange

Dr. Prange's thesis *"The War of Organizations – An Exploration of the Influence of Organization on the Success of Armed Forces in Hybrid Warfare"* provides a framework for methodically analyzing strategic security threats for large organizations that are faced with decentralized, highly adaptable aggressors. In his role as Research Fellow and Analyst at various think tanks he has briefed many senior members of staff on Capitol Hill on transatlantic political affairs, security policy, applied research desiderates on questions of strategic vulnerabilities in the cyber realm, conducting international corporate investigations. He is the Deputy District Chair for the Foreign and Defense Policy, Munich Working Group, and a member of the German Council on Foreign Relations (DGAP), German Atlantic Society (DAG), and the Clausewitz Network for Strategic Studies.

Andy Norton, Director Threat Intelligence, Lastline

Andy has been involved in cybersecurity best practice for over 20 years, specializing in establishing emerging security technologies at Symantec, Cisco and FireEye. In that time, he has presented threat and intelligence briefings for both Bush and Obama administrations, The Cabinet office, the Foreign and Commonwealth office, SWIFT, Swiss National Bank, Prudential Regulation Authority, the Bank of England, The Hong Kong Monetary Authority and NASA. Returning to Europe from Asia in 2011, he has spent the past 5 years helping many of the FTSE 250 companies measure, manage and respond to cyber incidents.

Lastline Corporate Headquarters
203 Redwood Shores Parkway, Suite 500
Redwood City, CA 94065

+1 877 671 3239
info@lastline.com
www.lastline.com

lastline™