The Driving Forces in Cyberspace are Changing the Reality of Security

Stonesoft Director of Cyber Security Dr. Jarno Limnéll and Dr. Jan Hanska.

We are moving towards a ubiquitous world where the border between kinetic and non-kinetic environments is becoming more blurred. Many aspects are merging into one, which we can interpret as the cyber domain. We are already living in an interconnected "online world", where we – as individuals, society, the military, and the global economy – rely on both the functionality and security of this "World of Bytes". Every second the cyber domain expands and becomes more complex. This means that there is an incredible scope of possibilities and the means develop new things. The integration of the online world with the physical world brings a new dimension to human life.

It is vital to understand that cyberspace should not be treated as a separate domain but as one that is entwined with the physical space.

In military terms, modern warfare demands the effective use of cyber, kinetic, and combined cyber and kinetic capabilities. Such capabilities could be an additional fifth domain in traditional warfare as the US military views it, or even a standalone approach to warfare. Cyber operations can be kinetic or non-kinetic. The boundaries between conventional and cyber operations are blurring, as cyber capabilities can be seen as a force multiplier in conventional operations. It should be noted that any future crisis will introduce cyber capabilities. They will have a cyber warfare component, whether it is public knowledge or not.

The purpose of this article is to describe and illustrate the differences between the laws of our real world and those concerning cyberspace. We argue that understanding the division between real and "cyber" is a mandatory prerequisite for understanding the essence of cyber threats, formulating suitable strategies and policies to counter

them, building required capabilities to militaries – and for survival and success in the ascending cyber world.

We argue that *the TSAAE (Time, Space, Anonymity, Asymmetry, Efficiency) formula* is among the most fundamental concepts that one must comprehend and take into account in order to be able to grasp the intricacies of cyberspace. Strictly defined, the TSAAE formula forms the nucleus of attribution. These are the driving forces that affect both the reality – and our understanding – of security. Without understanding TSAAE and without taking it into consideration strategic advantage can be lost, and one will not succeed in the new reality where “bytes” are increasingly important – especially where security is concerned.

If cyberspace was not connected – or had no ability to affect – the real world, we could leave it to the information management sector. But, because actions in cyberspace can potentially influence many aspects of our daily lives, it is too important to be treated in isolation. The IT community is full of specialists and often their thinking is driven by technological priorities. We need people from all sectors of human life: doctors, politicians, and business people – specialists with diverse expertise – to understand the basic characteristics of cyberspace and how it interfaces with their respective fields. In the real world, the nation state has a “monopoly of violence”. It is the only internationally recognized user of force on its own territory and is permitted certain forms of institutionalized violence to be able to carry out its responsibility to protect its citizens, whether it happens through the army, police, border guard and/or the judiciary system. In cyberspace, the state has not yet been able to assume a central role in regulating its citizens’ actions in cyberspace.

Common security comprehension of the demands of the digital age is vital for survival. In the digital world certain fundamental characteristics differ greatly from the material world. We highlight the TSAAE formula as key factors that need to be recognized to be able to function effectively in cyberspace.

We will proceed by illustrating the special qualities of the TSAAE factors one at a time and clarifying what the difference is when compared to the way these factors manifest themselves in the physical world.

Time

Time and temporality are irreplaceable parts of the human condition. There is a time for everything and everything takes time. Physical threats do not instantiate nor materialize in the physical world at once. In the world of bytes, it is different. The velocity of any cyber threat does not abide by the theories of mechanical movement,

but, instead, by the Einsteinian theory of relativity. A cyber threat is an initiated attack that moves at the speed of light. The choice of cyber weapon itself is immaterial – it is in electric form and coded in bytes. It can move through information networks and indeed, information itself can be a weapon. Thus, it is possible for a threat – or an attack – to actualize instantaneously via different vectors and angles of attack and decay.

Time, as a driving force in cyberspace, differs radically from the real world where it takes time to amass forces for an attack. Moreover, in this age of free-flowing information and satellites, it is very difficult to concentrate traditional forces for an attack without being observed and thus providing an early state of alert for the adversary. There are weapons, such as the intercontinental ballistic missile (ICBM) that can be launched at any given time from an aircraft, submarine or from a silo on the ground. But even these have a certain flight time until they reach their destination. Thus the attack will never come as a total surprise. In a state of high alert, a launch can be detected immediately, but there is still time to initiate counter-measures – or at least launch a counter-strike before the missile reaches its target.

It was primarily this concept that enabled nuclear deterrence to function. Despite the limited reaction time, the attacked party is able to launch their own missiles and this led to a policy occasionally referred to as mutual assured destruction or MAD. The potential destructivity of nuclear weapons led to a discussion about preemptive strikes in order to be able to prevent the destruction caused by the enemy striking first. Simultaneously, with the growth of nuclear arsenals by megatons, it was understood that even the one who struck first would be annihilated by the retaliatory attack. Fear of massive retaliation created deterrence and elevated the threshold of a nuclear attack. Still, the idea of preemptive strike lingered on in the theories of the classical nuclear strategists – coupled with measures that attempted to protect their own population by the means of nuclear shelters.

In the case of a cyber threat the question of a preemptive strike becomes even more acute. Even the short time that previously allowed reaction to an enemy attack by initiating retaliatory measures is nonexistent. Most rational minds abhor this idea of divining future actions of another state and striking “first” with highly destructive weapons. It leads to a paradox where actions are determined by morality and necessity. The argument “I won’t strike first unless you do” becomes prevalent.

On the other hand, the necessity of deterrence cannot rest solely on constant preparedness and the will to initiate an attack if hostile future cyber action is even suspected. Such a “mad dog” policy would be self-destructive because a state

practicing it would be seen an unpredictable and threatening. Thus, a cyber strategy that is too offensive might be counter-productive and likely to worsen the status of the player in the international community. Moreover, since responding to an attack before it takes effect is impossible due to the immediacy of a cyber attack to inflict its damage after it has commenced, a capacity to withstand attacks and remain functional must be built. Even though automation might create a suitable level of effective counter-measures and even provide deterrence, defensive models should stand on solid ground separated from offensive functions but in co-operation with them.

As to how the capacity to withstand attacks can be built, this depends on cyber strategy priorities. For the government of a networked society, the prospect of evading cyber threats by reducing connections – and diminishing society's network-related productivity – is not an option. The fear of cyber threats cannot force regression to the analog age. However, a foolproof cyber security system cannot be built – complete cyber security is a myth. It is not plausible to guarantee that any system connected to the internet cannot be breached. As long as an intruder possesses the skill, resources, will and incentive, a successful attack is a possibility.

Ultimately, there is no "ending" for networks. Thus, our information systems need to be built to be resilient – networks need enhanced capability to withstand attacks. Building a resilient network requires technical solutions. But the decision regarding how and where to seek a solution is a strategic one. One of the most important theories to implement with such solutions is to define the tactical depth and understand the movements possible within the known, potential battle space. This includes techniques, tactics and procedures, in both offense and defense capabilities.

Any player in cyberspace needs to demonstrate resilience – the capacity to withstand an attack and maintain the ability to function – as well as the capability to launch a retaliatory strike.

The immediacy of time from the commencement of an attack to its effects requires new measures for both cyber defense and offense. Traditionally thinking, and in contrast to threats in the physical world, there is no time to do anything when a cyber attack has begun. Similarly, the likely length of a cyber attack, or cyber war, is more comparable to estimations of an unlimited nuclear war than a drawn-out conventional war. Unless capabilities for cyber deterrence – in the form of ability to retaliate – and resilience are built in advance, the cyber attack will begin and end, with all its purposes fulfilled, before the defender can even properly notice that they are under attack, let alone protect against it.

The resilient maneuver for protection requires altering the digital battle space. The characteristics of cyberspace reintroduce the old martial fantasy of ending a war with one strike – the possibility of a truly lightning fast *Blitzkrieg*. Whether it is in the form of terrorism, industrial espionage or as part of armed aggression, the incredible speed of cyber attacks must be addressed in cyber strategy planning. *Tempus fugit* and our networked times need networked solutions. We no longer live in the agrarian or industrial age and thus our means of waging war need to reflect the societal development of our digital age.

This is not revolution, but a logical continuation of how our information-based society conducts most of its activities in the realm of cyberspace. Why should its wars or other forms of aggression be restricted to the traditional domains?

Space

Time and space are interwoven into a complex tapestry, the result of which is a bleak picture: no one is ultimately safe from an attack in cyberspace and, in turn, potentially any one can start an attack within the digital battle space. In the real world, geography has dictated the praxis of war and other uses of force. This had led to the fact that being located securely on the other side of the Atlantic and the Pacific Ocean from any potentially hostile state, the US has not faced a credible threat from either Europe or Asia in the sense that an actual war might take place on its continental territory. The distance to transport sufficient conventional troops into action has been too immense.

However, with cyber weapons, anyone can initiate an attack against any nation state at any time, instantly and from any part of the world. Depending on the demand, there is no need to calculate how long force concentration – that is, forming, equipping and training the troops necessary for an attack would require – nor are there delays in transporting troops. In the worst case, only the “enter” key needs to be hit and any location can be instantly under attack. In the interconnected world of cyberspace, geographical distance does not exist.

The question/challenge of space in the realm of cyberspace is related to where an attack may produce its effects – and also to where it can originate. The answer is: anywhere. A cyber attack against a US owned company or the government can originate just as easily from a PC in North Korea as from a Starbuck’s only a few blocks away from the target. An “army” in cyber warfare does not build up its forces in formations that can be detected by satellite. Instead, it might be comprised of one individual with enough skills and a laptop. A true weapon of digital mass destruction in cyber warfare can be carried in the real world on a memory stick, delivered in thousands to undefined geographical areas.

Since an attack is not connected to physical means – beyond a computer and an internet connection – it can be launched from anywhere. Furthermore, why should an attacker be restricted to using a computer in their home country? Today, it is easy to travel to the target country and use one of the free Wi-Fi networks that are available almost everywhere, as the platform for the attack.

Force concentration creates a high-level tactical and strategic issue for the defender and this is very difficult to overcome. A nation state may be occupied with foreign warfare capabilities long before any activities as such are conducted. These capabilities may lie dormant until action is requested and they can be disbanded within a moment's notice.

Confidence and Security Building Measures (CSBMs) that work in accordance with the conditions of the physical world are useless in cyberspace. There is no way to verify the capabilities of the potential opponent, or to detect a build-up of offensive measures. Thus, the potential enemy cannot be located and the switch from a potential to an actual enemy can occur unnoticed before it is too late. Naturally, it is possible, though difficult, to monitor, analyze and verify the cyber capabilities of nation states may develop in the future, but such developments would require international agreement and might still exclude multinational companies and other players in the business world. No matter how bindingly international law would restrict cyber policies, non-state actors in our Westphalian system are excluded from its jurisdiction and remain potential threats.

There is another aspect where the cyber domain differs from the real world. Conventionally, land territory is divided into nation-states that are recognized as such by other states. There are clear boundaries between nation states and where boundaries are contested, some kind of war or other crises are often present.

Cyberspace has no boundaries and there are no territorial divisions. While in the real world nation states enjoy complete sovereignty over their territory and population as well as a monopoly on violence, cyberspace is unclaimed territory that is free for all to exploit. Anyone, from individuals to groups of likeminded people, corporations and governments, can have the same role in cyberspace. Anyone can be a political player in cyberspace and there are no international laws or agreements that would restrict or guide their behavior since these apply traditionally in our international system only to states. Thus, in cyberspace, anyone can do practically anything.

This should not, however, lead to the folly of believing that one's actions in cyberspace have no repercussions in the real world. In a sense, the digital world and the real world overlap or, at the very least there is spillage from one to another. We have witnessed cyber capabilities influencing and causing damage in the physical real world. The effects shown where non-lethal but efficient in meeting their objectives.

Imagine similar attacks against the energy grid of a country within the northern hemisphere during winter. If there was no heating or electricity during severe cold weather in Canada, Scandinavia, a state like Michigan, or even a city like Moscow, what would be the death toll after a week's break in the service?

Furthermore, there is no guarantee that an aggressive action in cyberspace would not result in a response with conventional weapons. Indeed, it is even likely that should a cyber attack cause loss of life, retaliation would occur by means of military forces instead of computers – especially if the cyber capabilities of the state have been severely compromised or had not been sufficient even prior to the attack. A cyber attack that would result in casualties is viewed by the US as sufficient to justify kinetic means of retaliation. The two realms are not completely isolated and a significant part of deterrence in the cyber domain is related to the ability to respond to aggression with measures in the real world. Thus, intriguingly, the traditional offensive military capabilities a state possesses, simultaneously strengthens its cyber deterrence.

Cyber warfare does not abide by the laws of geography, whereby territorial divisions between nation states such as rivers, mountain ranges, or even oceans, can, to some degree, prevent damage from spreading. In addition, with modern precision weapons, it is possible to create "surgical strikes" that effectively restrict the range of damage caused. With cyber weapons, resultant impact is more difficult to determine and practically every cyber attack must be either a digital precision strike or have inbuilt mechanisms that prevent it from causing collateral damage. Otherwise, the networked nature of cyberspace might permit an uncontrollable spread of a virus, or even with a more sophisticated form of attack, create a situation where taking down some node or part of a network might render other parts of the network useless. Thus, initiating a powerful attack might result in an unplanned and unexpected outcome that may cause harm to the attacker, or even global damage, which would be intolerable to the international community. Thus, while a cyber attack can be initiated from anywhere, against anyone, it requires thorough planning to avoid damage escalation by transgressing networks.

Anonymity

Much of the recent discussion on the threat of cyber attacks has focused on the problem of attribution, which differentiates the logic of cyber warfare from other domains. Attribution can be defined as determining the identity or location of an attacker's intermediary thus turning it into more than just an anonymity clause. The ability to identify the source of a cyber attack is the basis for taking action against the attacks perpetrator. A response to a cyber attack is not possible without adequate attribution. Without attribution there is no fear of being caught, convicted and punished, thus it is tempting to use cyber weapons to conduct malicious activities.

In cyberspace, the attacker can remain anonymous when it supports the activity in question – and with this we are not referring to the specific group of "hacktivists" called Anonymous. Anyone can be an attacker and remain unidentified. In the real world, any act of direct aggression can be attributed to someone and someone may claim it for purposes involving typically a political aspect. In the digital world, attribution is difficult because there are not the obvious signs of a kinetic attack – and there is no physical evidence. Attacks can also be masked or routed through another country's networks.

Even if you are certain an attack came from a computer in a particular country, you cannot be sure the government is behind it. It is hard to deter if you cannot punish, and you cannot punish without knowing who is behind an attack. Moreover, hitting back against the wrong target not only weakens the logic of deterrence, it also creates a new enemy. This can be part of the tactical movements of an adversary: to allow watching a neighbor burning their house. This allows totally new players to engage in warfare formerly undertaken only by nation states and creates new models for strategies involved. A state with insufficient offensive capabilities may fall prey to digital terrorists who take advantage of the situation.

With a fist to the face in a barroom brawl – or a nuclear strike – an attacker can be identified. Furthermore, we usually have some forewarning or intelligence information about likely attacks by conventional means. We know who has the authority to initiate a nuclear strike in the US chain of command. Concerning conventional troops, we know who is in charge of what military unit and, consequently, we can follow the movement of those units. In other words, we know who might be the real world aggressors. After an attack it is easy to determine "whodunit" without being Sherlock Holmes.

In the cyber domain non-state would-be-aggressors are often relatively unknown beyond their own small circles of experts and the safest computer "whizz-kid" can turn from a harmless IT specialist into a "cyber general" at a moment's notice when

commencing an attack. However, these kinds of aggressors evidence little or no tactical understanding – at least for now. When a certain army unit is put into a state of high alert, its schedule changes and its activity increases and these indicators are easy to pick up. Many of the true experts in cyberspace spend a large amounts of their lives immersed in it and thus their daily pattern of life shows no outward change even if they are busy preparing an attack.

We must bear in mind that while designing and producing a cyber weapon requires expertise, using the selfsame weapon can be the epitome of simplicity. Before we can say there is a “cyber weapon” there must be a weapons platform to maneuver it. Truly anyone can commence an attack. Due to wireless networks with free access and the confusion of the meaning of space in cyber world, it is easy to ensure the anonymity of the attacker. Because “enslaved” computers from all around the world can be used in an attack, even in the aftermath it may be impossible to determine who indeed was behind the attack – in the case that the attacker has used all methods available for disguising his identity. Since the origin of the attack can be so arbitrary that it loses all meaning, blame cannot be placed on any nation state or other actor. Due to the ability to remain anonymous anyone can threaten and attack anyone else. The small can attack the big – and the meek are able to inherit the cyber realm.

The challenge of attributing cyber attacks raises some key questions: What is adequate attribution? How certain do we have to be about the identity of the attacker in order to launch counter-measures? Of course, the level to which one seeks attribution can vary significantly and depends on three interrelated factors: the desired sufficiency of attribution, the nature of the actions for which attribution is desired, and the intended purpose of the attribution. These are questions every nation has to answer while making their cyber strategies and doctrines.

At the same time, it is interesting to note that certain players, in order to achieve political advantage, have deliberately started to claim responsibility for conducting cyber attacks. This was the case with the legendary Stuxnet. The US government has unofficially admitted the attack in order to take credit for it – before the presidential elections. By admitting Stuxnet, the United States also demonstrated that it has the capability and willingness to use an advanced cyber weapon against an adversary. This is a strong message of deterrence. From the US the message is plausible, but it must be recognized that cyberspace is full of boasting concerning the capabilities of the players and until some demonstration of those capabilities has been given, these claims should be taken with a pinch of salt.

Asymmetry

Even though the original concept of asymmetry is very old, the applications of asymmetric warfare theories have been spreading to public discussions since the conflict between the US and al-Qaeda, highlighted by the 9/11 attacks. In this conflict, with limited resources to attack the US, al-Qaeda employed asymmetrical warfare tactics by using hijacked airplanes to attack vital targets in the US.

Asymmetric warfare exploits the weakest point of an opponent and attempts to uses competitive advantages in an optimal way. Asymmetric warfare is the war between combatants whose relative power and/or strategies or tactics differ significantly. Asymmetry is something the weak resort to in order to be able to counter the stronger on their own terms.

The cyber domain creates new possibilities for asymmetric warfare. All cyber operations, including information warfare, are asymmetric by nature, whilst delivery and introduction may be symmetric. Big brains are more important than big guns. In the cyber domain, it does not matter how many people or pieces of equipment you have – instead, expertise and capabilities determine the result. Cyber attacks are asymmetric because they may be perpetrated by few upon many with limited cost and resources.

Compared to the physical world, the barriers to entry in the cyber domain are much lower. In the physical world, governments have a monopoly on the large-scale use of force and stronger states dominate the weaker ones. No one would dream of attacking Russia, China, or the US by conventional means. To launch a cyber attack, all a person needs is a computer, an internet connection and technological knowledge.

Cyberspace enables greater malicious potential at lower cost than any other domain. A small number of highly trained programmers using commercial off-the-shelf equipment can develop lethal tools and deploy them with great effect. Moreover, in most countries today the dependence on complex networked systems for the support of military and economic activities creates new vulnerabilities that can be exploited by hostile actors. Currently, the asymmetric nature of cyber warfare creates an issue of manpower-on-demand. Performing efficient defense or offense requires a vast amount of manpower and resources in intelligence, information exploitation, delivery and operational picture management – including other pillars of cyber warfare. It can be fairly said that efficient performance does not scale easily without manpower. There is, however, an ongoing change towards automation and platformization.

Because of the asymmetric nature of cyberspace, cyber capabilities will reduce power differentiators among states. The largest powers are unlikely to be able to dominate cyberspace to the same extent they have dominated other domains, such as sea and air. Strength in cyberspace does not have to equate with material resources, vast territory, access to seas and high level of population. These are some of the sources of power according to classical geopolitics. Cyberspace provides smaller states and non-state actors with the opportunity to create (if they are innovative and possess enough knowledge) capabilities that the major players might or might not have in sufficient quantity and quality to be competitive. In the digital world the intellectual resources of the state dominate and material resources diminish in importance.

This will affect the power balance in the world, at least to some extent. Power diffusion is increasing the ability of non-state actors to inflict harm. Both smaller states and non-state actors can play a more significant role in international cyber conflicts than they have ever done in the physical world. However, it is important to notice that sophisticated attacks against high value targets, such as defense communications systems, require a higher cost of attack, which involves large intelligence agencies to intrude physically and/or crack highly encrypted codes – as illustrated by Stuxnet. This had such complex structure that it could not have been manufactured without a relatively extensive team of experts. Thus, the relative reduction of power differentials is not the same as equalization – large governments will still have more resources. This does not refer only to a percentage of GNP used on military purposes, but how a state's intelligence community is structured and how it allocates its resources. It is cheaper to build a high level of cyber warfare capabilities that to air-mechanize an army.

Another important point with regard to asymmetry is the advantage of the attacker. In the cyber domain offense currently dominates defense. Current circumstances are more conducive to attackers than defenders. This leads to new and complex dimensions in national security policies. States that traditionally have focused on policies and methods aimed only on self-defense must seriously consider adopting offensive cyber capabilities and shape their policies accordingly. The defender faces an asymmetric strategic challenge because the actual question is one of vulnerabilities.

The logic of cyber vulnerability is pre-emptive: the vulnerability of your opponent is your asset and, in order to know what your asset is, you have to look for your opponent's vulnerability. Cyber attacks are not enabled by the generation of force but by the exploitation of the enemy's vulnerabilities. The cyber domain strongly favors offense because so many vulnerabilities exist and an attacker does not have to have a

"quantitative superiority" for an attack to be successful – as you must have in the physical world. The defender must be able to perform counter-actions, which require an in-depth understanding of digital battle space and both one's own assets and liabilities. A cyber attack allows for a successful delivery of payload if only one among millions of attack attempts finds just one crucial vulnerability that can be judged as a hit on target. While governments derive power from greater resources, they lose power to greater vulnerability in their infrastructure. In situations of reciprocal dependence, asymmetrical vulnerability produces power, and in the cyber domain, performers benefit from asymmetrical vulnerability compared to governments and large organizations.

In the cyber domain, in the sense of asymmetry, it is much easier to hide your materials. In fact, you do not even need a factory, military base or physical materials. The development of cyber weapons is very difficult to "see". It could be taking place in the room next to you, and you are unlikely to know about it. At the same time, it is worth understanding that the lifespan of a kinetic weapon can be years while a particular cyber weapon is only useful for as long as the vulnerability in the target system remains in place. Once the vulnerability has been patched, the weapon becomes useless, at least against that specific target. Thus, again, the situation is asymmetric. Cyber weapons must be developed in secret and are in essence a "one-use-only" kind of weapon. Therefore intelligence and information exploitation, automation, and modeling of attacks are priorities in tasking. Their existence is a carefully guarded secret. It is difficult to defend against a weapon you have not seen in action, or if you have not been warned of the vulnerability that it is intended to exploit.

Efficiency

Based on the combined effect of all the aforementioned characteristics, the potential efficiency of a cyber attack against a networked society can be something unprecedented. Cyber warfare and its theories resonate harmoniously with those of nuclear warfare. However, an all-out or even a restricted nuclear war between two states armed with these weapons of mass destruction never broke out. Common sense and survival instincts prevented this. Thus, even with cyber, we should not get into doomsday scenarios. In fact, scenarios can be difficult to define at all due the potential amount of them.

The term "effective cyber attack" by no means translates into the proverbial "take down" of the internet. On the contrary, such attacks might involve intrusions into unprotected networks for the purpose of compromising data tables, degrading communications, interrupting commerce, or impairing critical infrastructures (such as transportation or medical and emergency services) in a way that undermines trust at

the expense of a smoothly running economy and society. A key component of efficiency is the potential of the attacker to do a legion of things simultaneously, parallel, in combination, with a variety of vectors of attack, and with the speed of light.

The more a society has chosen to integrate its functions with data networks, the more it should attempt to protect these networks and the wealth of information contained therein. Societies that strictly integrate their decision-making, accounting for information assets, such as the registry or delivery of information, are encountering the most yield in such matters.

The hard truth is that perfect cyber security is a myth – and the current situation favors an offensive approach over a defensive one. The defender faces an asymmetric strategic challenge. Cyber offense can be very cheap. Defensive measures are expensive, but they are no match for the economic damage that can be inflicted if security measures are not in place. In addition, the attacker faces an asymmetric strategic challenge if the defender dominates its digital warfare playground combining assets and liabilities and the tactical depth of defense, allowing altering the rules of game efficiently with tactical moves and performance over adversary.

We will never know the potential of cyber weapons before they are used. And once a weapon has been identified and analyzed, it often becomes useless very quickly since the vulnerabilities it exploited are located and addressed. Furthermore, in the broad sense, “cyber” includes all kinds of information attacks, including ideological wars. In the case of the Arab Spring, the cyber dimension was about well-planned and large-scale campaigns by the masterminds of unrest. It was closer to an information warfare operation showdown than an exercise of technical ability – nor did it adhere to the romantic notion of citizens deprived of their democratic freedoms spontaneously rising to demand them and using social media as their chosen medium of communication. We should not restrict the cyber domain only to the world of computers but include the potential for propaganda and strategic communications as well.

To understand the scope of a cyber threat, we must recognize the discrepancies between the topography and geography of the digital world and the real world. Mountains and oceans are hard to move, but portions of the cyber domain can be turned on and off with the flick of a switch. The real world is set in stone, and geographical alterations occur slowly, but continental drift is instant in a cyberspace that is constantly in flux. What it is today only implies what it could be tomorrow.

Cyber capabilities can be built by anyone. They are not restricted to traditional great powers or even other states. Non-state actors can cause strategic effects in two

critical ways: firstly, they can make advanced capabilities available for purchase and employ them either through cooperation with some state or via internet underground non-state actors. Secondly, non-state actors can form unholy alliances where states provide advanced capabilities to them directly while retaining plausible deniability. The commercialization of security – hiring private defense contractors to the dirty work – is already a part of state policy in many parts of our real world. Why would the digital world not follow suit? Plausible deniability and the difficulty of attributing cyber attacks leads actors to disregard the possibility of retaliation and to use cyber attacks against adversaries they would not dare to attack with conventional weapons. Possible misattribution on the part of the target of the attack, coupled with the possibility of subsequent escalation, will lead to an increased frequency of war.

The cyber domain is artificial, created by human beings using hardware and software. Any actions that a combatant takes in that world require the movement or manipulation of data – but it is not only a question of bytes. There are direct implications for the physical world – via the TSAAE formula presented in this paper.

How we think about cyberspace influences the way people create meanings for their experiences in the real world. For example, can we still claim that being friends requires anything more than a relationship built in cyberspace? Networked structures in cyberspace create similar networks between individuals, businesses etc. Society – “the real world” – must seize the initiative in shaping cyberspace otherwise cyberspace will reshape us. And since we, as citizens, are not masters of this reshaping and it does not work through democratic channels, there is the risk that our real world society will assume a form we would not like it to have. Man must be the master of the machines and the networks.

To make an allegory: fire was a factor that enabled societal development when man controlled it. Yet, numerous great cities have been devastated by fire when it was not under man’s control anymore. Interestingly, current developments in cyber warfare capabilities are blurring the role of decision-making on the tactical level. In the case of responding to an attack, the demands for efficiency and immediacy practically require automated processes and this distances cyber war procedures from the people waging it. Occasionally efficiency spells automation. Another, even more direct and tangible means of influence results from the direct inter-linkage of the physical and digital domains. Due to automated, computer-controlled systems the real and digital worlds now overlap. Just as a hacker creates a bridge for influencing cyberspace, a virus can influence the real world by creating a malfunction in a real world system. Thus, a cyber threat can kill in real life.

The most destructive possibilities, US Defense Secretary Leon Panetta has said, involve “cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack”. He described the collective result as a “cyber Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability”. Cyberspace is unpredictable and self-developing. Thus, cyber threats are polymorphic, multi-faceted and intangible. They can materialize out of nowhere, anywhere, at any time and may not adhere to logic. This is due to the fact that the laws and causality of cyberspace differ from the reality around us. We perceive and interpret this reality though the lenses of the human condition while computers and their networks are logical and emotions are replaced by cold rationality.

People will make the difference to cyber security

We – the whole world – are becoming more dependent on the “world of bytes”, and its security. At this moment it seems that cyberspace is the new “wild, wild, west” where the lone gunmen prowl at large and are colored with a certain romantic twist of “sticking it to the man”. The man, however, is able to exploit cyberspace better than individuals even if they work through a collective, such as Anonymous. We need an iconoclast to rid us of such romantic notions. All too often the ability of Anonymous to bring huge multinational companies to their knees is lauded and admired and not a moment’s thought is given to the notion that their capabilities could be redirected for even more malign purposes. The mask should be torn to reveal the potential threat for everyone beneath it. The more meaning cyberspace has for nations, the more potentially damaging to everybody it becomes. The more developed a society is, the more vulnerable its vital functions are to a cyber attack and thus the potential efficiency of an attack increases progressively.

The formula of TSAAE illustrates the need for new security understanding and a new approach to security issues. The cyberspace environment is dynamic to the extreme and, in order to succeed in it, dynamic actions and security solutions are needed. The existence of vulnerabilities does not justify cyber-attacks, but makes them much more tempting to attackers, and unfortunately new vulnerabilities and threats emerge on a daily basis. Technology is developing so rapidly that anything written today will become obsolete when printed. Thus, the means and ways of cyber offense and defense should be left to the technically talented, to be employed and specifically tailored for each situation. It is the purposes and goals of such functions that need to be formulated by the politicians.

Strategies for survival and success in cyberspace are needed and cyber capabilities are already an integral part of policy – even if the majority of citizens do not perceive

them as such. Cyberspace activities do not form a continuation of politics. They are a part of political process and can pervade the system just as thoroughly or superficially as demands set for them dictate and the resources of the nation state allow.

Technological solutions involved in cyber warfare will soon be soon mature enough to be seen as weapons platforms, and while all technology plays an important role in the cyber domain, automated systems increase in importance as the requirement for speed is emphasized. Because the systems have grown both efficient and complex, automation is here to stay and there is no turning back. Yet, the human has to reign over the machine and the automated system remains a tool. It is not and should not be technology that will win the day on 21st century cyber battlefields. In past military operations and exercises it is the people that have made the difference and so it will remain in the future. The question is whether we as humans are capable to maintain the amount of discipline and efficiency needed in our decisions.

Just as perfect security eludes us in the physical world, there is no perfect security in cyberspace, and there never will be. But our goal should be to minimize the threats at an acceptable cost and enable the continued advances that the information age has heralded so far. In order to do that, we have to understand the Driving Forces of security in cyberspace. We have to comprehend how each of the TSAAE factors differs from its physical world manifestation and what these differences require from the cyber strategies we are currently developing. To counter the demands set by these differences is to enhance security and diminish the likelihood of cyber attacks. In terms of security the complexities of our societies demand just as complex and comprehensive solutions and a formula like TSAAE helps focus attention on the critical factors. Cyberspace is not all about threats and vulnerabilities. It opens up new vistas for those bold enough to embrace opportunities. And we will.

About Stonesoft

Stonesoft Corporation (NASDAQ OMX: SFT1V) delivers proven, innovative solutions that simplify network security management for even the most complex network environments. The Stonesoft platform unifies management of entire networks – including Stonesoft and third-party devices – blending integrated threat management, end-to-end high availability and network optimization into a centrally controlled system. As a result, Stonesoft provides the highest levels of proactive control, always-on connectivity and compliance at the lowest total cost of ownership (TCO) on the market today. Founded in 1990, the company is an established leader in network security innovation with corporate headquarters in Helsinki, Finland and Americas headquarters in Atlanta, Georgia. For more information, visit http://www.stonesoft.com