# Cyber-Attacks as coercive instruments

*by Hrafn Steiner*

**Resumé**

Efter IT attackerna mot Estland under 2007 samt Iran 2010 har intresset för IT-krigföring ökat markant bland både akademiker och beslutsfattare. Utanför ramarna om vad som tekniskt är möjligt är det viktigt att förstå hur denna form av attacker kan användas som verktyg politiskt. Denna studie söker förklaringar till nyttjandet av IT attacker genom att tillämpa teorier om tvingande diplomati (*coercive diplomacy*) i fyra uppmärksammade fall av cyberkrigsföring. Även om mycket fortfarande är osäkert beträffande de fyra händelserna står det klart att cyberattacker kan och kommer att bli ett flitigt använt verktyg i framtida konflikter.

NUMEROUS ATTEMPTS HAVE been made to explain cyber-attacks from existing frameworks of political conflict. It has been labelled 6th generation warfare, hybrid warfare and other similar terms. Sceptics have questioned the feasibility and proponents have argued for its potential. Whether or not cyberwar is a real threat to national security now or in the future, it is undeniable that these attacks keep occurring in connection with political conflicts.

Over the years the debate has mainly focused on whether cyber-attacks constitute an act of war or not. Many of the debaters have based their arguments on Clausewitz's classical formulation of war: war is political, war is instrumental and war is violent.[1] Amongst them is Professor Thomas Rid who argues that cyber conflicts lack key elements of warfare, and, in particular, that they are not violent. Those who argue that cyber war indeed falls within the scope of war, counter that Rid makes many unmotivated assumptions when defining war and the relationship between force, violence and lethality.[2]

In the article from 1993, 'Cyberwar is coming!', John Arquilla and David Ronfeldt argue that progress in information technology will change how society handles conflicts and warfare.[3] Further, they theorize that future wars will take place, in part, in the digital arena.[4] Over recent years their thesis seems to be gaining support by the increasing use of information technology in political conflicts. As society becomes more reliant on IT infrastructure security experts and politicians are becoming increasingly concerned with this new source of vulnerability, and the risk that information and communication technology (ICT) could be used for military purposes. The exploitation of weaknesses in systems or computer networks (hacking) and malicious computer code (computer viruses) has evolved from a nuisance, with potential economic damage, into a threat to national security.

Two decades after writing 'Cyberwar is coming!', Arquilla revisited his earlier speculations on cyberwar in a new article.[5] Here he observes that cyberwarfare is on the rise, although not entirely in the way he and Ronfeldt had anticipated. Arquilla points to three incidents as major watershed events in the evolution of cyberwar. The first two came in 2007 and 2008 when Estonia and, later, Georgia were attacked by systematic cyber-attacks in the wake of conflicts with Russia. These events made it difficult to

deny the relevance of the cyber domain in modern conflicts.

Many countries, among them Russia and the USA, have adopted defence policies which indicate that cyber-attacks are considered an armed assault on their territory.[6] Further, many states have formed their own cyber-warfare units, indicating that cyber-attacks are considered a military matter and are at least perceived as a tool of force. The concept of cyberwar has been heavily debated as attempts are made to categorize this threat into evolving definitions of generational warfare, yet little attention has been given to the impact of cyber-attacks on political decision-making.[7] Winston Churchill once said: "However beautiful the strategy, you should occasionally look at the results." Many texts outline the possibilities and probable dangers with cyber-attacks, although little attention has been given to critically examine the effects of cyberwarfare. By studying contemporary theories on the use of political force, one can begin to understand the ways in which cyber-attacks can harm society and pose a threat to national security.

This article will apply the theory of coercive diplomacy on politically motivated cyber-attacks in order to examine the possibility that cyber-attacks may be used as an instrument for political coercion as well as their potential efficacy.

## Defining and measuring coercive diplomacy

In the *Arms and Influence* political scientist Thomas Schelling discusses the use of force during inter-state conflict. The result of military action usually leaves destruction and suffering in its wake. The cost of a military operation will always be both economic and emotional. Harm, pain and suffering cannot be disregarded; this undeniable fact of armed struggle will affect all parties in a conflict to a lesser or larger extent; therefore decision-makers will strive to avoid drawing harm, pain and suffering upon their own population and upon themselves. With this knowledge, a nation can instill and build upon the fear of harm in order to compel its opponents into giving in to demands before engaging in full-scale war. Schelling considers the use of suffering as a tool for political persuasion, *coercive diplomacy,* as opposed to traditional warfare, which he calls *brute force*.[8]

While brute force seeks to overcome the enemies' strength, coercive diplomacy seeks to influence the enemies' motives. By using suffering as a coercive tool the goal of military strategy no longer strives to defeat the enemy in combat, but instead persuades the enemy that refusing to adhere to demands will be too costly. Shelling compares this to the difference between taking what you want and making someone give you the same thing.[9] Having established the essence of coercive diplomacy, it is necessary to understand the mechanism of coercive diplomacy. How does coercive diplomacy work in practice?

Authors Daniel Byman and Matthew Waxman focus on the mechanism and instruments of coercive diplomacy. They note that causing suffering alone does not necessarily have a coercive effect. Suffering must be dealt in such a way that the hardship has a political effect.[10] The targeted vulnerability must be perceived as impact-full enough that the nation will go out of its way to avoid damage. These *pressure points* vary from nation to nation and are dependent on a variety of factors such as the form of government, economic, health, and diplomatic relations, etcetera. A prominent difference is between democratic and autocratic governments, where the latter can to a greater degree disregard the opinions of the public.

It is also important to note that pressure points are political and psychological in nature; the most important factor is the *perception* of vulnerability, not *de facto* vulnerability.

Byman and Waxman also argue that coercive diplomacy should not be viewed as a single political action where a state issues a threat and another state reacts to that threat by resisting-failed coercion or backing down- successful coercion.[11] Instead, coercive diplomacy needs to be viewed as a succession of moves and countermoves in a dynamic process between two parties in conflict. A coerced nation will not simply accept the threat but move to minimize the impact of the threat. This can be done in two different ways: one can either negate the effect of the threat or impose a greater cost for the coercing nation to execute the threat. This *dynamic process* of coercive diplomacy makes it harder to determine the effect of a single action. A coercive act will prompt the target state to counteract by submitting to the demands or responding with an alternate coercive move. Coercion is a dynamic contest with both actors often employing intimidation tactics over time.[12]

There are two key elements of coercive diplomacy: the *instruments* used to apply pressure on a target nation and the targeted *mechanism* on which the instruments are applied. Suggested instruments include: sanctions, isolation, support for insurgency, air strikes, invasions, land grabs, and threats of nuclear attack. Some instruments, such as air strikes and land grabs, present a theoretical problem. The aim of coercive diplomacy is, according to Schelling, the avoidance of brute force. Byman and Waxman acknowledge this and conclude that the lines between brute force and coercive diplomacy can be blurry. The main difference between coercive diplomacy and brute force is in the motivation of the attacker. Brute force is used when it is perceived that negotiations will go nowhere. In these instances, the military objectives are independent of the target nations' counter moves. With brute force there are no political actions the target nations can undertake in order to stave off the attacks, except unconditional surrender. However, if the aim is to use the invasion to exert political pressure, the act should be considered as being coercive diplomacy, not brute force.[13]

Coercers seldom rely on one sole instrument to achieve their goal. Combinations of the tools are used in the dynamic process, as outlined above. These instruments are employed when the coercer hopes to exploit one or several mechanisms in order to prompt concession. The way to implement effective coercive diplomacy is to increase the threatened costs to the adversary, while denying opportunity to either negate those costs or counter-escalate. Byman and Waxman call this *escalation dominance*. In order to attain escalation dominance the coercing nation must identify areas that are sensitive to the adversary, and then effectively threaten in a manner which the targeted nation cannot avoid or protect against.

Other factors that favour coercive diplomacy are outlined in *Forceful Persuasion*, written by Alexander L George in 1997.[14] In the book he lists seven conditions which favours, but will not guarantee, successful coercive diplomacy.[15]

*Clarity of objective* – The consistency of demands conveyed to the target give clear instructions to follow in order to avoid punishment.

*Strength of motivation* – In order to convey a credible threat it is essential for the coercing power to be sufficiently motivated by what it perceives to be at stake.

*Asymmetry of motivation* – Because coercive diplomacy is a clash of interests, motiva-

tion will be two-sided. Coercive diplomacy only works if the effects of giving in to the demands are perceived as less harmful. The advantage of ignoring the demands may very well be deemed high enough to endure any threatened punishment.

*Sense of urgency* – The coercing power needs to generate a sense of urgency for compliance in order to motivate the target to comply.

*Domestic as well as international support* – Various examples highlight the fact that domestic as well as international support for a cause, or at least a lack of open opposition to the policies, contribute to the credibility of the issued threats.

*Unacceptable escalation* – More than simply achieving escalation dominance, the escalation alone must be regarded by the target as unacceptable.

*Clarity concerning the precise terms of settlement of the crisis* – It may be necessary to establish procedures and terms for the cessation of hostilities and safeguards to insure that no further aggressive acts will be performed by the coercing party.

## The logic of cyber-coercion

The available cases of politically motivated cyber-attacks are few and use of the instrument is in its infancy. A major problem in researching cyberwar is the problem of attribution. As stated above, cyber-attacks are seldom attributed with 100 % certainly to a specific actor, despite the fact that a plausible suspect is often quickly identified. However, attribution is not as important as it may first seem.

Byman and Waxman outlined cases where coercion is not perpetrated by the principal actor but can also be performed by allies and other actors sympathetic to one's cause. The question of attribution can be circumvented by disregarding the actual perpetrator and focusing instead on which party gained and which party suffered from the act. Using allies is not uncommon in coercive diplomacy;[16] it may even be to the advantage of an actor that the origin of the attack remains unclear, as long as the demand is effectively conveyed. Counter-escalation is harder to achieve if the attacker is unknown, and plausible deniability may have a deterring effect on the target's ability to counter the attack or motivate counter-moves against its allies.

By focusing on the demands (whether explicit or implied), the gaining party can be determined without establishing who initiated the attack. The key component of coercive diplomacy is the use of force in order to create, or potentially create, suffering; a situation which the adversary wishes to avoid. There is no need for violence or lethality, as long as the actions inspire the adversary to attempt avoidance of the threatened effect. Any tool capable of inflicting suffering, whether in the form of death, destruction or any other cost, can therefore be considered a tool of coercive diplomacy. If a deliberate act results in suffering for an adversary, it is thus a potential tool of coercive diplomacy.

For this study, coercive diplomacy is understood as every action wherein the use of force is employed to compel an adversary to change political decision-making before attempting to convey any demands as opposed to instigating a full scale war, which maintains the goal of rendering the enemy incapable of fighting.

Cyber-attacks can therefore be employed in two different manners: first in the conventional sense as a tool for warfare or limited strikes, and secondly as an independent tool for coercive diplomacy. The question is whether the latter is comparable to the first.

For this essay the main question posed is whether cyber-attacks fit the prerequisites for a coercive instrument, and how well they function. Four cases were selected for this study: the DDoS (Distributed Denial of Service) attacks on Georgia, as well as Estonia, the Israeli air force strike on Syria's nuclear weapons programme in 2007 and the 2012 Stuxnet attack against the Iranian programme. In the cases of Georgia and Syria, cyber-attacks were used in combination with kinetic force in order to act as a force multiplier; in the cases of Estonia and Iran cyber-attacks were the primary method of offensive actions employed by the attacker.

The limited availability of material and cases to study creates difficulties in using an approach with a more extensive scope. Therefore, this analysis may be regarded as a pilot study with findings significant and useful for further research.

## Case studies

### Cyber-attacks on Estonia in 2007

After the declaration of independence in 1991, the russification of Estonian culture was perceived as a threat to Estonian independence and Estonian officials have created legislation with the aim of minimizing Russian influence in the country.[17]

In 2004, Estonia took further steps away from Russian influence, when the country gained entry into both the EU and NATO. However, Russia still retains significant, though primarily economic, interests in Estonia, e g Estonia is a key country for Russian exports of gas and oil to Europe.[18] For Russia the integration of Estonia into the EU and NATO is both a political and economic problem as the Baltic is perceived as part of the Russian sphere of interest and Estonia is leading the region away from Russian influence.[19]

Estonia has made immense efforts to adapt the country to western standards. Information Technology is a field where Estonia has become a global leader. The Estonians rely heavily on the Internet for many aspects of critical infrastructure; everything from financial transactions to water supply is controlled via cyberspace,[20] 97 % of bank transactions are online and 60 % of the population use the Internet in their daily life. Government bureaucracy is highly dependent on information technology; the IT director at the Estonian Ministry of Defence, Mihkel Tammet, refers to the government operations as a "paperless government".[21]

In April 2007, Estonian officials decided to move a Soviet era bronze statue, honouring Soviet soldiers killed during World War II, from the centre of Tallinn (the capital of Estonia), to a military cemetery outside the city. For Estonians, the statue was a painful symbol of Soviet occupation, but ethnic Russians still living in Estonia saw it as a move to further marginalize the Russian-speaking population. This move sparked widespread protests.[22] Riots broke out between Russian protestors and Estonian police, resulting in multiple injuries and the death of one protester. The Kremlin came to the defence of the Russian diaspora and called the moving of the statue a violation of Russian rights. They imposed sanctions on Estonia and briefly shut down the railway line between Tallinn and St. Petersburg.[23]

As the physical protests died down in the streets, the conflict moved to cyber-space. On 9 May, Russia celebrates the defeat of Nazi Germany. The same day Estonian IT infrastructure was subjected to several large-scale DDoS cyber-attacks. Detailed instructions where spread in Russian language online forums detailing how users could participate in the offensive. Thousands of computers were involved in the attack.[24] Some participating

computers belonged to pro-Russian activists while others belonged to bot-nets, unknowing users whose computers had been infected by a malicious code. This enabled the attackers to use the computers for their own gain.[25] It is estimated that the networks funnelled traffic up to 1,000 times the normal amount, causing Estonian Internet infra-structure to collapse and effectively shutting down most Estonian IT services.[26] Attacks continued for nine days with a final extensive attack on 18 May. Many institutions reported minor disturbances after that date. The attacks effectively prevented bank transactions and even the use of teller machines to withdraw cash. Only a handful of financial institutions published figures of estimated losses, though for one bank the loss amounted to millions of dollars.[27]

There is little doubt that the attacks on Estonian websites were connected to the overall tension between the Russian minority and the Estonian government, but experts have failed to produce credible evidence that supports claims that the Russian government was directly involved in the attack. However, many experts in the field point out that the magnitude of the attack would have been impossible if there were not at least some form of coordination and preparation.[28] One of several groups claiming responsibility for the attacks was the Nashi (Russian for "ours"). Nashi is a pro-Putin group organizing 120,000 Russian youths between 17 and 25. While not part of the Russian government, there are many links between it and the youth group. The assistant of then parliamentary leader Sergei Markov, was the leader of Nashi and openly confirmed his group's participation in the attacks.[29]

Whatever their involvement in the cyber-attacks, Russia played a key role in mobilizing the activists and ensuring that tension remained high. Many experts are far from convinced that the Russian government had nothing to do with the attacks. A NATO official is quoted as saying: "I won't point fingers. But these were not things done by a few individuals. This clearly bore the hallmarks of something concerted. The Estonians are not alone with this problem. It really is a serious issue for the alliance as a whole".[30]

To counter the cyber-attacks, Estonia received help from the EU and NATO Computer Emergency Response Teams (CERT), who contributed to restoring the networks to normal operation. At the same time, NATO and EU officials began to discuss strategies and policies regarding response to cyber-attacks. The result was a unified NATO policy on cyber-defence, but despite German calls for extending Article 5 of the NATO charter to cyberspace, the organization decided against adopting a unified policy treating a cyber-attack as an armed assault.[31]

## Cyber-attacks and limited warfare in Georgia in 2008

Georgia is, like Estonia, another former republic within the USSR. In 1921 the Red Army invaded the country, toppling the government to install a communist government loyal to Moscow. However, opposition to the occupation has remained strong since that time. This has resulted in several protests that were violently put down by Soviet troops, the latest one in 1989. In 1991, shortly before the collapse of the Soviet Union, Georgia declared its independence. Following that event, relations with Russia have been characterized by mutual distrust and tension (German, 2009). Since the disintegration of the Soviet Union in 1991, the South Caucasus region has become a battleground for geopolitical influence. The main opposing forces are Russia, who strives to maintain its influence,

Turkey and Iran, as well as Western powers seeking to establish influence in the wake of the Soviet collapse.[32]

Following the 2003 "Rose Revolution", Georgia's President Mikheil Saakashvili has been more inclined to seek partnership with Western organizations such as the EU, NATO and ISCE. Integration with both NATO and the EU have been key priorities for the Georgian government, evident in the country's National Security Concept, approved by parliament in 2006.[33]

Russia aims to maintain its influence in the South Caucasus, and opposes Georgia's pro-Western tendencies.[34] Russian president Vladimir Putin has insisted that former Soviet states are part of the Russian sphere of interest and has opposed Western entanglement in what he considers the Russian "strategic backyard".[35] As part of its heritage as a former Soviet state Georgia retains a close dependency on Russia for export and trade; something Russian policy makers have exploited to exert economic pressure on the country. Economic intimidation has proved a successful way of exerting pressure on Georgian civilians, in addition to undermining the government. In 2006 this became evident as Russia imposed a ban on Georgian food exports to Russia. This resulted in a collapse of the Georgian wine market which exports up to 87 % of its produce to Russia. Furthermore, Georgia was, until late 2008, heavily dependent on imports of Russian gas.[36]

Seeds for what would culminate into the August 2008 hostilities were planted six months prior in the wake of the EU and US recognition of independence of Kosovo. Russia, an ally of Serbia, was not pleased with the outcome and retaliated by stating that it would recognize the separatist regions of Georgia as a counter-move. Russian anger deepened when earlier, during the NATO Bucharest Summit in April, it became evident that Georgia, together with Ukraine, had made substantial progress with negotiations regarding membership in the military alliance.[37] As a response, Russia increased its cooperation with the separatist regions, establishing direct official Russian relations with the South Ossetian and Abkhaz authorities.

This situation slowly deteriorated until July 2008, when Georgian villages and military installations where attacked by separatist militia, provoking several serious clashes between Georgian military and separatist militias.[38] Volunteers arriving from Russia were integrated into the standing South Ossetian militia, with little or no reaction from Russia; thus prompting Georgia to accuse Russia of complicity and involvement by proxy.[39] On August 8, confrontations spilled over into open conflict with separatist militia prompting Russia to send in its own troops to assist the separatists. After three days of open combat between Georgian and Russian military forces, Georgia was forced to withdraw from South Ossetian territory.[40]

Parallel to the ground assault, Georgian ICT infrastructure was subjected to several cyber-attacks. On 19 July observers noted the first of several substantial DDoS attacks directed towards Georgian governmental presence on the internet. The DDoS attacks were also accompanied with the defacement of government websites. The attacks escalated in severity until, on 10 August, the Georgian government found themselves barely able to communicate via the Internet. This was due to the fact that the whole Georgian ICT infrastructure had come to a standstill.[41]

The immediate results were devastating for the Georgian regime. Unable to communicate with the civilian population, government coordination was hindered during the Russian advances. While there are no official links

between the cyber-attacks on Georgian ICT infrastructure and Russia, the DDoS attacks on Georgia mirrored the Russian combat operation in the land-warfare domain; major military advances would often coincide with major DDoS attacks on Georgian ICT infrastructure.[42]

On 12 August, a ceasefire accord was brokered between Russia and Georgia by French president Nikolas Sarkozy. Then Russian president Medvedev declared an end to the Russian offensive, yet ordered his troops to remain. Russian military were given instructions to destroy "pockets of resistance", as well as other aggressive actions and the Russian government reserved the right to undertake additional security measures they deemed necessary. Broad buffer zones where established and unilaterally determined by Moscow, drawn up to inconvenience the Georgians. Some examples encompassed the inclusion of the only road connecting Eastern and Western Georgia, the Senaki airfield and the entrances to the harbour of Poti; all of whom would now be under direct Russian control.[43]

## Cyber-attack on the Natanz 2010–2012

Together with allied Western powers, Israel and the USA suspected that Iran had re-established its nuclear weapons programme and had been pursuing nuclear weapon capabilities since the mid-1980s. The claim had been repeatedly denied by Iranian officials, who insisted that the Iranian nuclear programme was for civilian use only, in accordance with the non-proliferation treaty.[44] While it was not perceived as likely that Iran would attempt to use nuclear arms against Israel, the proliferation of nuclear arms might embolden Iran, and Israeli officials feared that the nuclear arms might end up in the possession[45] of more radical non-state actors. Israel views a nuclear Iran as a potential existential threat and a threat to Israel.[46]

A possible strike on Iran had long been debated and in 2004 Israel procured F-16 warplanes, specially built for long range missions, which would put possible Iranian nuclear installations within Israeli operational reach.[47] A potential military strike on Iranian nuclear research would have to overcome several difficulties: (1) a military strike could have a rallying effect on the Iranian regime, strengthening it; (2) Iranian nuclear facilities would be harder to reach than Syria and Iraq since Israel would have to fly over several hostile countries; (3) Iranian nuclear infrastructure is more developed than in both Iraq and Syria, creating a resilience factor greater than that held by the other two countries (4) The political fallout of an attack against Iran would worsen the already tense relationship with other Arab countries; (5) Iran might withdraw from the NPT treaty, which would limit international oversight; (6) Iranian capacity to retaliate is stronger than that of Iraq and Syria.[48]

Nuclear weapons require uranium where the ratio of isotopes with a larger mass than normal is higher. In order to produce highly enriched uranium, Uranium hexafluoride is injected into centrifuges to separate the heavier isotope from lower yields. The facility necessary for this process is located near the city of Natanz, Iran, in an underground complex containing a few thousand fast rotating centrifuges.[49]

In late 2009 a Russian IT-security company, Kaspersky Labs, discovered the first sample of a Trojan virus called Stuxnet.[50] Once Stuxnet had infected a computer it began to search for predetermined programs used for controlling machinery.[51] One target program of the virus, called Simatric WinCC Step7, was the software used to control motors,

valves and switches in industrial systems, in this case the uranium enrichment turbines.[52] While most malicious computer codes aim at spreading their payload as widely as possible, Stuxnet differed in that respect. The designers put extensive effort into ensuring that the virus only attacked very specific computer environments, limiting the attack to a single manufacturer and even downloading the precise model numbers from the hardware the program controlled in order to verify that it was on target.[53]

When the correct conditions on a computer were found, the worm delivered its actual payload. The virus did two things; first it took over the monitoring system which supervised the turbines whose purpose was to alert staff of any irregularities. Instead of sending an accurate report of what was actually going on with the turbines, the monitoring system would convey what the worm had instructed it to report; that everything was working satisfactorily. Even if a technician performed a routine check, the monitoring system would report everything as normal. Secondly, it altered the code handling the acceleration of the centrifuges causing them to spin irregularly by accelerating and decelerating the centrifuges repeatedly.[54]

The resulting stress was devastating for the centrifuges. The IAEA requires plants handling enrichment to make their decommissioned centrifuges available for inspection to see that no radioactive material is smuggled out. Under normal circumstances, around 10 % of centrifuges were exchanged annually. The facility in Natanz held approximately 8,700 centrifuges, making 800 replacements per year a normal turnaround cycle. Yet in 2010, within a few months, between 1,000 and 2,000 centrifuges had to be swapped due to structural damage.[55]

When IT specialists discovered the worm, they were perplexed by its complexity. The worm used previously unknown weaknesses, known as zero-day vulnerabilities, in the source code of different computer systems to propagate and deliver its payload. Antivirus researchers examine more than 12 million pieces of malware per year; normally fewer than a dozen manage to exploit a zero-day vulnerability.[56] Stuxnet alone exploited four such vulnerabilities.[57] Symantec, an IT security company, determined that it had been necessary for the attackers to set up their own mirrored environment, including their own turbines, in order to program the virus in this manner; making this an unlikely product of a non-state actor. In all likelihood the code was written by at least five different technicians with expert knowledge in distinct fields, suitable for the design of the virus.[58]

## Airstrikes on Al-Kibar 2007

Bashar Assad succeeded his father as president of Syria in July 2000. The young newly elected president initiated several actions which worried the Israeli intelligence community. He supplied weapons to Hezbollah in Lebanon, received high ranking officials from North Korea, and his rhetoric was perceived as more unpredictable than his father's.[59]

In 2006, Israeli intelligence experienced a breakthrough when they managed to install a Trojan virus on a senior official's computer while he visited Great Britain.[60] This program was designed to give access to computers without permission. On the computer they discovered colour photographs and documents indicating that the Syrians were constructing a secret plutonium reactor in the Syrian desert.[61] Concerned about the possibility of a hostile country with nuclear capabilities, the Israelis consulted the U.S. for a joint strike on the facility. The U.S. was reluctant to repeat the scenario in

Iraq, where weapons of mass destruction had been one of the primary arguments for the attack. Therefore, they preferred placing pressure on Assad in other ways.[62] The Israelis were convinced that any talks would allow Assad to buy time to acquire necessary components; they believed that a limited strike was the only way to stop the program. The US would not be part of an attack, but agreed not to leak any information or block an Israeli operation, "Olmert did not ask Bush for a green light, but Bush did not give Olmert a red light".[63]

Just after midnight on September 6, 2007, fighter jets originating from Israel headed north-east across the Syrian border and dropped their payload on half built installations hidden in the desert before returning home.[64] In the aftermath of the raid, security researchers and experts questioned how the Israeli strike force was able to penetrate Syrian airspace without any response from the Syrian air command nor from its newly purchased air defence batteries.[65] Eventually, it became apparent that Syrian air radar systems had failed to report the intrusion of any single aircraft. As far as the radar system was concerned, no penetration had occurred.

Preceding the Israeli airstrike, a stealthy UAV (unmanned aerial vehicle) was sent towards the Syrian border and into the air defence radar beam. Each time the UAV was hit by the Syrian radar systems, a small packet of information was sent into the direction of the beam, thus piggybacking onto the signals bouncing from the radar station. The piggyback signal contained a specially crafted virus, designed to communicate a false radar image later the same day. This report coincided with the planned Israeli airstrike. By the time the Israeli force struck, there was no chance for the Syrians to comprehend what had happened before the fighter jets were on their way home.[66]

The initial response from Syria was that Israel had penetrated its airspace and dropped bombs in the desert, but without managing to cause any structural harm or human casualties.[67] Israeli and American officials kept quiet, declining to comment to the media. It would take almost a year, until April 2008, before Israel and USA publicly confirmed the intended targets, a North Korean-constructed nuclear reactor. The U.S. and Israel suspected these facilities were to be used for manufacturing nuclear weapons.[68] It was similar to a North Korean reactor well suited for plutonium production.[69]

The reactor itself was far from the only key element needed for nuclear weapons production. Syria lacked several key components for the capability to produce nuclear weapons. They still needed fuel for the reactor to produce plutonium and without a reprocessing facility, which was not available at the Al-Kibar facility, extracting the plutonium from the spent fuel would have been impossible.[70] The strike negated approximately six years' worth of work, the average time it takes to build a similar reactor as in Al-Kibar.[71] The raid also complicated the programme by triggering intensive investigations from the IAEA regarding Syria's nuclear programme.[72]

Before the Al-Kibar attack Syrian activity was, for the most part, unsuspected and the facility unknown. In May 2008, the IAEA informed Syria of its intentions to send inspectors to investigate the site at Al-Kibar and review available information. Syria agreed to the demands of the IAEA and provided unrestricted access to the site during the visit in June 2008. The IAEA concluded that the site was "similar to what may be found in connection with a reactor site".[73] It criticized the U.S. and Israel for not notifying the IAEA of their findings, instead deciding to act in-

dependently. The use of force undermined the due process of verification and rule of law.[74] One IAEA diplomat indicated that the IAEA took the findings seriously, due to the fact that Syria was on the agenda right behind Iran and North Korea.[75] Another consequence of the attack is that there are indications that North Korea was less eager to help the Assad regime after the attack.[76] The Israelis had reached their goal without costing them in the manner of a traditional attack.

## Conclusions: Cyber-attacks and political coercion

The goal of this paper is to delaminate if, and how, cyber-attacks can be used as a tool for political coercion. Two types of cases have been studied: two wherein cyber-attacks were the main means of coercion and two where cyber-attacks facilitated the use of kinetic force. This is, in itself, nothing new. Electronic warfare has been a part of armed conflict for decades, and as the military adopts ICT so will electronic warfare. The question relevant for this paper is whether stand-alone cyber-attacks can be used as a tool for political coercion in the same manner.

In the first case studied of a cyber-attack on Estonia, there is evidence that the cyber-attacks resulted in substantial costs both in the form of damage to the systems and in the form of loss of potential profit while the economic system was in deadlock. The few sources that reported indicated a significant cost and the political fallout was massive. In Georgia, both the economic sanctions that preceded the hostilities, as well as the subsequent invasion and land grabs, inflicted substantial costs and suffering. Byman and Waxman suggest that weakening or debilitating the country as a whole is effective for countries with leaders held responsible for the care and wellbeing of the country as a whole.[77] In the second case of cyber-attacks, Stuxnet, exact costs are harder to estimate. The virus did damage the enrichment turbines increasing the overhead costs. These costs, however, are not comparable to the costs of a total destruction of the facility, as in the case of Al-Kibar. Both cases where cyber-attacks were employed show, in different aspects, that a cyber-attack can be used to inflict costs on a target nation in a similar way as other coercive instruments.

In the case of Estonia there is clear evidence that the attack weakened the country as a whole and initiated, or at least facilitated unrest amongst the Russian minority. It can also be said that the attacks showed that NATO was incapable of protecting its member states from a similar attack, possibly prompting countries like Ukraine and Georgia to question whether joining the alliance was beneficial. In that case it can also be said that the attack was a form of power base erosion aimed at NATO.

The attacks on Georgia triggered similar mechanisms. It can be argued that weakening and power-base erosion were employed in a similar way as in Estonia. In the case of Georgia, Russians also managed to deny Georgia political and military victory when they successfully thwarted their attempts to integrate the separatist regions of South Ossetia and Abkhazia.

In the case of Iran and Syria the subsequent attacks could have been aimed at denying the respective target the continuation of their nuclear enrichment programme. In the case of Syria, the attacks may also have made North Korea more hesitant to cooperate, eliminating a key ally in Syria's attempt to acquire nuclear technology. This same offensive appears to have effectively ended the Syrian nuclear weapons programme, but Iran has, so far, shown no sign that the strike

has affected the regime's resolve to continue. Though it may have succeeded in causing delay and has cast an uncomfortable light onto the Iranian programme, the nuclear proliferation was already under IAEA scrutiny; as opposed to Syria, where the attack led to renewed interest from the IAEA.

Both Estonia and Iran show evidence of cyber-attacks inflicting costs on the adversary in such a way that mechanisms of coercion where triggered; this prompted response from the political decision-makers. It is therefore possible to conclude that cyber-attacks fit the pattern determined by literature to be classed as instruments of coercive diplomacy.

The second issue to address is efficacy of this tool. There is some evidence to suggest that several of the criteria of coercive diplomacy suggested by George were fulfilled when the coercer used cyber-attacks, as presented in a summary table below. Notable, however, is the lack of apparent escalation or any clarity regarding the terms of settlement.

As noted above, George stated seven factors for successful coercion but many of those conditions were found to be lacking in the studied cases, especially when analyzing the actions where stand-alone cyber-attacks were used.

The targeted nation needs to understand what is demanded and how to act in order to avoid punishment; the case of Estonia lacks this clarity. The Russian government and protesters conveyed demands ranging from "don't move the statue" to "don't marginalize the Russian minority". There are also varying theories for implied demands, challenging NATO alliance sovereignty over the Baltic region.[78]

For Iran and Syria, the overall objective was clear: termination of the nuclear enrichment programmes and/or nuclear weapons production. All of the tested cases show considerable strength of motivation.

The DDoS attacks where unprecedented in strength, coordinating thousands of hacktivists in the attacks. The Stuxnet worm was groundbreaking in its complexity. The designers of the software had invested many resources in order to make the programme as potent as possible. In the cases of Georgia and Syria, both Israel and Russia showed the targeted nations that they were prepared to use force in order to achieve their goals.

The attacks on Estonia and Georgia clearly conveyed a sense of urgency for the political elite to act. Estonia, who prided itself in being a paperless society, suddenly ground to a halt; politicians and security experts were unable to thwart the attack, while Georgia faced imminent Russian invasion and military defeat. In the case of Stuxnet, it is harder to discern a sense of urgency. In all likelihood technicians and scientists working at the plant faced considerable stress while managing increased failures; however, there are no indications that a sense of urgency was conveyed to the political decision-makers. That was also the case in Syria, where no evidence suggested that other actions would follow the attack. Substantial time passed before details emerged enough for the IAEA to inquire into the matter.

Evidence of the opponent's fear of unacceptable escalation exists in Georgia, but there are no attestations that Estonia or Iran feared immediate escalation following the attacks. In the case of Georgia, the government felt pressured to consent to an armistice agreement with Russia, thus giving Russia far-reaching freedom of action, possibly due to fear of unacceptable escalation. In the case of Syria, there might have been fear of escalation, but this study has not found any accounts supporting that idea. One significant aspect of cyberwar is the lack of direct attribution of the attacks. Both studied cases retained plausible deni-

ability and were therefore characterized by the lack of any direct communication of terms or demands. Georgia is the only case examined, which included precise terms of settlement.

The examples of attacks on Estonia, Iran and Syria all are characterized by the lack of direct negotiations between the conflicting parties.

The findings, depicted above as a summary in Table 1, show that cyber-attacks did not support evidence that a majority of factors that George established for effective coercive diplomacy were fulfilled. Neither did comparing the cyber-attacks with similar cases, where other coercive instruments where implemented, show that cyber-attacks fulfilled at least the same or corresponding criteria. This raises the question of why cyber-attacks would be favoured over other coercive instruments.

## Why cyber-attacks?

Faced with many alternatives for coercion, one fundamental question is why cyber-attacks are used at all. While there is little doubt that cyber-attacks *can* be used as coercive instruments, this study finds no evidence that cyber-attacks are more *effective* instruments than other coercive tools. The justification for use of cyber-attacks must therefore be found in other constraints.

The Stuxnet attack and the attack on Al-Kibar share many similarities. Both attacks were perpetrated (to some degree) by Israel and the U.S. and both aimed at denying other regimes in the Middle East the ability to obtain nuclear weapons. In the case of Al-Kibar, the Syrian nuclear research programme seems to have been halted, as opposed to the outcome in Iran. As suggested in theory, the effects of coercion might backfire prompting the targeted nation to defend its stance more furiously in the light of the attack.

The case of Estonia and Georgia share many similarities: both are countries that are former Soviet republics, both countries are in Europe and both countries have a large Russian- speaking minority. The difference is that Estonia is far more integrated into the European Union and NATO than Georgia. Both conflicts revolved around the influence of Russia or Russian minorities in the country. Neither conflict seems to have affected the aim of the political elite to further integrate their respective country into both NATO and EU. In the case of Estonia, that work is already done and the cyber-attacks do not seem to have affected political decision-making for Russian interests in a favourable manner.

*Summary:*

| **Factors favoring successful coercion:** | **Targeted nations:** | | | |
|---|---|---|---|---|
| | **Estonia** | **Georgia** | **Iran** | **Syria** |
| Clarity of objective | No | Yes | Yes | Yes |
| Strength of motivation | Yes | Yes | Yes | Yes |
| Asymmetry of motivation | No | No | Plausible | Yes |
| Sense of urgency | Yes | Yes | No | No |
| Adequate domestic and international support | Yes | Yes | Yes | Yes |
| Opponents fear of unacceptable escalation | No | Yes | No | Yes |
| Clarity concerning precise terms of settlement of the crisis | No | No | No | No |

*Table 1. Summary of George factors for successful coercive diplomacy in the discussed cases.*

Georgia is still in the process of entering both the EU and NATO, although it is possible that the conflict was successful in halting the process, as nearly six years have passed since the Bucharest Summit, where Georgia, together with Ukraine, were declared likely future NATO members.

Both the cyber-attacks and the Russo-Georgian war might not have been intended against the attacked countries, but aimed at a wider audience. Alternately, the intent could have been to warn countries perceived to be within the Russian sphere of interest, the goal being to alert them of the consequences of distancing themselves from Russia, which neither NATO nor the EU could protect them from.[79]

Coercive diplomacy is a dynamic process and the end result of the studied cases may not be realized for years to come. As with other diplomatic activities it will take years before any certain conclusions can be drawn about the long-term effects of cyber-attacks on political decision-making. Comparing cases involving coercive diplomacy in a methodically satisfying way is therefore problematic.

There are simply too many factors to allow for isolation of the relevant considerations. The results described in this article do not conclusively answer the question if cyber-attacks are more or less effective than other coercive instruments. However, when comparing the cases an interesting pattern can be discerned: both cases of the studied cyber-attacks, although similar to the instances where kinetic force was employed, exhibited significant disadvantages and high risks with military action such as invasion, land grabs or air strikes. The lack of attribution limits the overt connection between a threat and action and therefore seems to curb the response to the attack. Issuing a threat publicly puts pressure on a regime to respond to that warning in order to remain credible. A regime might find that the political cost of resisting the ultimatum might be less than the cost of meeting the demands, causing a coercion to backfire and locking the target into its opposition.

In the case of the attack on Al-Kibar, major concerns lay in how Syria would retaliate; Israel undertook measures in order to minimize the risk and scope of a potential retaliation. Attacking Natanz with a cyber-weapon sparked limited overt response from Iran, as the initial lack of attribution made it hard for Iran to respond in the initial phase with force. The same can be said for the case of Georgia and Estonia. Estonia is part of the NATO alliance and enjoys the protection of Article 5 of the NATO charter. A limited strike, as in the case of Georgia, would have compelled other NATO partners to respond with force, an escalation Russia probably preferred to avoid. NATO is trusted to shield Estonia from Russian invasion; however, it could not hinder Russian-sympathetic hackers from an attack over the Internet. Comparably, for the Stuxnet offensive, many political analysts assert that, should air strikes have been used, Iran would have been compelled to counter-escalate with a military response rather than bend to the will of Israel and the U.S. The Iranian safeguards which discouraged an air strike, had no impact on the risk of cyber-attacks on the country.

Cyber-attacks work because they target distinct vulnerabilities other than those of other coercive instruments. The lack of security in IT infrastructure creates vulnerability in countries which otherwise have enough protection to deter coercing attempts. Reports warning of the dangers of cyber-attacks as political tools are plentiful, but scientific study of the political use of cyber-attacks is limited. More descriptive research on the use of cyber-attacks for political reasons needs

to be done before any conclusions can be drawn. Because cyber-attacks can be used as instruments for coercive diplomacy and the problem with attribution makes it hard to retaliate, this option may be an appealing instrument when military or other overt actions are undesirable. In that regard, the high cost-effectiveness of this strategy can be expected to increase the incidences of cyber-attacks used as coercive diplomacy in the future. Many nations invest in defensive and offensive cyber capabilities and therefore the use of cyber-attacks is likely to increase in the wake of political conflict.

This article has found that factors other than those established by George matter when coercive strategy is determined. The factors established by George cannot determine what effective coercive diplomacy is, and the author makes no attempt to establish his list as either necessary or complete in order to evaluate the productiveness. Better tools for evaluating the effect of forceful persuasion, taking into account the dynamic process of coercive diplomacy, need to be developed. Cyberwar might, as Rid claimed, never happen, but that does not preclude the possibility that cyber-attacks will be a serious concern for national security.

The author studies political science with a focus on security policy. The essay is a revised edition of his Batchelor thesis.

## Notes

1. Howard, Michael; Peter Paret and Rosalie West: *Carl Von Clausewitz: On War*, Princeton University Press, 1984, pp.102-114.
2. Stone, John: "Cyberwar will take place", *Journal of Strategic Studies*, Vol. 36 (1), 2013, pp. 101-108, and McGraw, Gary: "Cyber war is inevitable (unless we build security in)", *Journal of Strategic Studies*, Vol. 36(1), 2013, pp. 109-119.
3. Arquilla, John and David Ronfeldt: "Cyberwar is coming!" *Comparative Strategy*, Vol.12 (2), 1993, pp. 141-165.
4. Ibid.
5. Arquilla, John: "Twenty years of cyberwar", *Journal of military Ethics*, Vol. 12 (6), 2013, pp. 80-87.
6. *The Department of Defense Cyber Strategy*, Department of defense, Report, Pentagon, Washington 2015.
7. Se for example: Reed, Donald J.: "Beyond the War on Terror: Into the Fifth Generation of War and Conflict", *Studies in Conflict & Terrorism*, Vol. 31 (8), 2008, pp. 684-722 and Liles, Samuel: "Cyber warfare compared to fourth and fifth generation warfare as applied to the Internet," *2007 IEEE International Symposium on Technology and Society*, IEEE, Las Vegas, 2007, pp. 1-3.
8. Schelling, C. Thomas: *Arms and influence,* Yale University Press, New Haven 2008 [1966].
9. Ibid.
10. Byman, Daniel and Waxman, Matthew: *The dynamics of Coersion,*Cambridge University Press, Cambridge 2002, p. 27.
11. Ibid.
12. Ibid., p. 37.
13. Ibid.
14. George, Alexander L.: *Forceful persuasion: coercive diplomacy as an alternative to war,* United States Institute of Peace Press, Washington D.C. 1997.
15. Ibid., pp 75.80.
16. Op. cit. Byman, Daniel and Waxman, Matthew, see note 10, pp 152-155.
17. Herzog, Stephen: "Revisiting the Estonican Cyber attacks: Digital threats and miltinationas responses", *Journal of Strategic Security,* Vol. 4 (2), 2011, p. 50.
18. Ibid., p. 53.
19. Puheloinen, Ari: *Russia's Geopolitical Interests in the Baltic Area,* National Defence Collage of Finnland, Helsinki 1999.
20. Op. cit. Herzog, Stephen, see note 17, p. 51.

21. Ibid.
22. Ibid.
23. Ibid.
24. Ibid.
25. Wilson, Clay: *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress,* Library of Congress, Congressional Research Service, Washington DC 2008.
26. Ibid.
27. Op. cit. Herzog, Stephen, see note 17, p. 52.
28. Ibid.
29. Singer, Peter W. and Allan Friedman: *Cybersecurity and cyberwar : what everyone needs to know*, Oxford University Press, New York 2014.
30. Traynor, Ian: *Russia Accused of Unleashing Cyberwar to Disable Estonia,The guardian,* 2007-04-17, http://www.theguardian.com/world/2007/may/17/topstories3.russia, (2014-10-07).
31. Op. cit. Herzog, Stephen, see note 17.
32. German, Tracey: "David and Goliath: Georgia and Russia's Coersive Diplomacy", *Defence Studies,* Vol. 9 (2), 2009, pp. 224-241.
33. Ibid., p. 226.
34. Ibid.
35. Ibid., p. 229.
36. Ibid.
37. Ibid.
38. Allison, Roy: "Russia resurgent? Moscow's campaign to coerce Georgia to Peace", *International Affairs*, Vol. 84 (6), 2008, pp. 1145–1171.
39. Ibid.
40. Ibid.
41. Korns, Stephen W. and Kastenberg, Joshua E.: "Georgia's cyber left hook." *Parameters*, Vol. 38 (4), 2008, pp. 60-76.
42. Hollis, David M.: "Cyberwar case study: Georgia 2008" *Small Wars Journal*, 2011-01-06, *http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.* (2014-08-18)
43. Ibid.
44. Bahgat, Gawdat: "Nuclear Proliferation: The Islamic Republic of Iran", *Iranian Studies*, Vol. 39 (3), 2006, pp. 307-327.
45. Ibid.
46. Ibid.
47. Ibid.
48. Ibid.
49. Rydqvist, John and Zetterlund, Kristina: C*onsequences of military Actions Against Iran,*Försvarets Forsningsinstitut, FOI, Stockholm 2008.
50. Falliere, Nicolas, Murchu, O Liam and Chien, Eric: *W32.Stuxnet Dossier. White paper,* Symantec Corp., Security Response, Cupertino 2011.
51. Ibid.
52. Zetter, Kim: "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History", *Wired,* 2011-07-11, *http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet.* (2014-07-17)
53. Langner, Ralph: "Stuxnet: Dissecting a cyberwarfare weapon." *Security & Privacy (rev 1.4)*, IEEE, Vol. 9 (3), 2011, pp. 49-51.
54. Op. cit. Falliere, Nicolas; Murchu, O. Liam and Chien, Eric, see note 50.
55. Ibid.
56. Ibid.
57. Murchu, Liam O.: "stuxnet using three additional zero-day vulnerabilities", 2010-09-14, *http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities.* (2014-10-18)
58. Op. cit. Bahgat, Gawdat, see note 44.
59. Follath, Erich, and Holger Stark: "How Israel Destroyed Syria's Al Kibar Nuclear Reactor", *Der Speigel*, 2009-02-11, *http://www.spiegel.de/international/world/0,1518,658663,00.html.* (2014-10-18)
60. Ibid.
61. Ibid.
62. Makovsky, David: "The silent strike", *The New Yorker,* 2012-09-17.
63. Ibid.
64. Garwood-Gowers, Andrew: "Israel's airstrike on Syria's Al-Kibar facility: a test for the doctrine of pre-emptive self-defence?" *Journal of Conflict and Security Law*, Vol. 16 (2), 2011, pp. 263-291.
65. Clarke, Richard A: *Cyber War.* Harper Collins, New York 2010.
66. Ibid.
67. Op. cit. Garwood-Gowers, Andrew, see note 64.
68. Ibid.
69. Kreps, Sara E. and Fuhrmann, Matthew: "Attacking the Atom: Does Bombing Nuclear Facilities Affect Proliferation?" *Journal of Strategic Studies,* Vol. 34 (2), 2011, pp. 161-187.
70. Ibid.
71. Ibid.
72. Ibid.

73. *Implementation of the NPT Safeguards Agreement in the Syrian Arab Republic,* IAEA Board of Governors, Vienna 2013.
74. Op. cit. Garwood-Gowers, Andrew, see note 64.
75. McEclroy, Damien: "Uranium Found in Syria by UN Nuclear Inspectors", *The Telegraph,* 2008-11-10, *http://www.telegraph.co.uk/news/worldnews/middleeast/syria/3418686/Uranium-found-in-Syria-by-UN-nuclear-inspectors.html.* (2014-08-14)
76. Op. cit. Kreps, Sara E. and Fuhrmann, Matthew, see note 69.
77. Op. cit. Byman, Daniel and Waxman, Matthew, see note 10.
78. Op. cit. Herzog, Stephen, see note 17.
79. Op. cit. German, Tracey, see note 33.