# Impact of Alleged Russian Cyber Attacks

*By William C. Ashmore*[*]

During a two week period in April and May of 2007 Estonia was the victim of a sustained massive cyber attack on its information infrastructure. While the cyber attack was not the first nor was it the largest, it was the first cyber attack that was directed at the national security of a country. (Davis, 2009)

The significance of a cyber attack on a small country can be difficult to measure for a casual observer. Estonia is a small country that can be seen as a model for the future. Estonians have developed and used internet technology for voting, education, security and banking (ninety-five percent of banking operations are done electronically) (Collier, 2007). It is not uncommon to see a sign for free Wi-Fi internet access at a pub, restaurant or on public transportation.[1]

Imagine going to an Automated Teller Machine (ATM), while on a business trip, to get money for meals and lodging and the system is down. Restaurants and hotels are unable to process your credit card. You try to send a message to your bank, your work, and your family but the computer servers are all down. The government is unable to communicate with the public and its different departments. News agencies are having difficulties publishing information. The aftermath of a cyber attack can impact anyone that uses the internet, whether it is an individual, business, or government that has been affected. By investigating the attack, how it happened, and Estonia's reaction, states can decide whether their internet defences and strategies are adequate.[2]

The cyber attacks on Estonia have implications for both its allies and adversaries. This article is not meant to establish a complete strategy for cyber defence but to create a better understanding of how a cyber attack can have far reaching consequences beyond the immediate aftermath of a targeted infrastructure. What are the implications for Estonia? Is the framework of the North Atlantic Treaty Organization (NATO) appropriate for cyber defence? Is an attack against one really an attack

[*] William C. Ashmore is a Major in U.S. Army.

against all? Does the Organization for Security and Co-operation in Europe (OSCE) have the ability to react to cyber attacks? Lastly, does the Russian Federation have a coherent cyber strategy that it is willing to use and what have been the consequences for Russia?

Any country that uses the internet as part of its infrastructure needs to be aware of the vulnerabilities and consequences of a cyber attack on their system. A coherent strategy must include internet defences that are set-up in conjunction with technical defences. Currently, legal definitions for cyber crimes do not exist in all countries. The international community must examine treaties and update them to better define assistance and common defence in the event of a cyber attack. Russians have shown the ability and the desire to use cyber warfare. Cyber strategy by, in defence of, or against Russia affects more than computer networks. Although, attacks that originate in China, Japan or the United States may have similar implications they are outside of the scope of this article.

Internet attacks occur on a daily basis throughout the world. How nations prepare themselves for an internet attack will determine the impact of a cyber attack on their infrastructure. The aim of this article is to achieve a greater understanding of the possible Russian cyber strategy and to understand the counter measures that can be used to prevent or mitigate cyber attacks. This awareness could possibly prevent a tactical defeat during conflict when a cyber attack targeting command and control and communications infrastructure is blocked.

## 1. The media accounts

Internet trade magazines and mass media reports were used to gather evidence on the events surrounding the cyber attack on Estonia. Internet sources were a major source of information on the subject of cyber security because of the amount of information that is new and has not yet been published in books. Several Estonian government officials have spoken on the issue of cyber attacks at great lengths. Estonian government documents were also used to analyze the Estonian response to the cyber attack. Media accounts along with documents from the North Atlantic Treaty Organization (NATO) and the Organization for Security and Co-operation in Europe (OSCE) were used to analyze the aftermath of the Estonian cyber attack on organizations and other states. Analysis of Russian involvement was conducted using western documents.

In order to understand the reasons behind the Estonian cyber attack this article will explore the social tensions and the cyber attack itself. The impact that the attack had on the different actors will also be noted. The reality of the attacks indicates some important implications for Estonia and other former Soviet satellites to work with NATO to develop a coherent cyber strategy. Russia's cyber strategy also has considerable significance for the United States. This article will conclude with a summary of possible countermeasures to a cyber attack.

## 2. Cyber attack on Estonia

The social tensions between Estonians and Estonia's Russian minority are key to understanding why there was a cyber attack. Estonia is made up of 1.3 million people where 25.6 percent of the population is Russian (Central Intelligence Agency, 2008). In 1918, the Estonians gained their independence from Russia, and in 1940 they were forced into the Soviet Union. From 1940 until they regained their independence in 1991 Estonia viewed Russia's presence as an illegal occupation. Mass deportations were made, people were summarily executed, and the population was resettled by ethnic Russians. Russians on the other hand view the Estonians as ungrateful because they were saved by Russians from the Nazi German fascists. Today there exists significant animosity between the Russians and the Estonians that permeate personal relationships and political interactions within the country and between the two nations. (Vesilind, 2008)[3]

The actual events that occurred in Estonia centred on the Soviet Bronze Soldier monument. The Bronze Soldier monument is a World War II Soviet War memorial which memorialized the graves of Soviet Soldiers who died during World War II. However, over time ethnic Russians had used the memorial as a rallying site for demonstrations and other forms of protest against the Estonian government. This led to a decision by the Estonian government to move the monument to an area that was less public. (Davis, 2009)

The decision to move the statue led to actual riots in the capital city of Tallinn on April 27th, 2007. The demonstrations degraded into criminal activities involving looting and the destruction of private and public property. Hundreds of demonstrators were arrested, most of whom were ethnic Russians. The civil unrest was contained, order was restored to the streets by the Estonian government, and most of the physical damage was repaired by the next morning. (Davis, 2009)

During this period of civil unrest computers in the Estonian government and the Estonian national media were hacked into with significant affect. Some of the attacks on the system were vandalism of sites and some were distributed denial of service attacks (a cyber attack that disrupts internet service so that a user cannot access a given computer service). The attacks started small with a major attack culminating on the Estonian internet system on May 9th, 2007. This date coincidentally corresponded to the day the Russians celebrate their victory over the Germans in World War II. During this time a Russian youth-group conducted protests against the Estonian ambassador to Russia and against the Estonian Embassy in Moscow. The protests against the ambassador and the embassy did not end until the ambassador left the country as part of a deal that was negotiated by Germany. The Russian government even suspended passenger rail services between Tallinn and St. Petersburg. The riots, the protests, the stopping of rail service, and the cyber attacks led to an increasingly tense relationship between Estonia and Russia. (Davis, 2009; Kampmark, 2003: 288-293)

The Estonians were able to respond to the cyber attacks in a very proficient manner, as they were able to coordinate responses that only caused relatively short term outages instead of any permanent damage to their IT infrastructure. The Estonian government was able to employ its Computer Emergency Response Team (CERT) which coordinated IT responses among government and civilian specialists. However, due to the ambiguous nature of the internet and the use of fake internet protocol (IP) addresses the Estonian's were unable to conclusively prove who initiated the cyber attacks. (Collier, 2007)

The cyber attacks themselves were not very sophisticated as the attackers used techniques that had been in existence for several years. The focus of the cyber attack was to completely shut down the IT structure of Estonia. The cyber attackers used botnet attacks to perform a distributed denial of service rendering systems that use the internet useless. Botnets are hijacked computers that send out mass amounts of information which overwhelm an internet server. The increase in internet traffic will cause a server to exceed its bandwidth capabilities and cause it to shut down. The botnets can be installed well in advance of a planned cyber attack, and they can be placed in any computer anywhere in the world. If the computer user has not installed appropriate protective software on their computer they will not even know that they have been hijacked and that they are participating in a cyber attack. The botnet attacks on the Estonian IT structure ended as abruptly as they began leading Estonian officials to conclude that the attack was a planned and coordinated. (Davis, 2009)

The cyber attacks on Estonia illustrates the vulnerability of IT structures that rely on the internet. The use of technology can improve personal, business, and government interactions but it is still vulnerable to attacks and interruptions. The next section of this article will concentrate on the implications for Estonia in the aftermath of the cyber attacks.

## 3. Implications for Estonia

After the cyber attacks in 2007, there were several implications for Estonia as the country recovered from the cyber wake-up call. Some implications had an immediate impact on the people and the government of Estonia, while others were more long term and required a deliberate strategy. The immediate implication for Estonia was the loss of services for government, communication, and banking. What emerged from the attack was Estonia's ability to counter and minimize the effects of the attack. There was no permanent damage to the information technology (IT) structure and financial losses were minimal, but the significance was frightening. (Collier, 2007)

One of the long term implications is the continued strain on Estonia's relationship with Russia. Members of the Estonian government and outside observers believe that the attacks originated in Russia, but that fact remains unproven. The finger pointing between Estonia and Russia began immediately after the attacks and continues today. Dmitry Peskov, Deputy Press Secretary for the Russian President said, "Russia can no way be involved in cyber terrorism and all claims to the contrary are an absolute lie" (The Baltic Times, 2007a). Andrus Ansip, the Estonian Prime Minister, and others have accused the Russian government because of the identification of Russian internet protocol (IP) addresses used in the attack. To date, Russian involvement has never been proven, but the implications and belief that they were involved continues to influence and affect the relationship between Russia and Estonia. (The Baltic Times, 2007b)

After the attacks and recovery, Estonia has been heralded as a leader in technological security. According to Alexander Ntok, head of Corporate Strategy at the International Telecommunication Union, "it was imaginative responses that allowed Estonia to emerge from the spring cyber attack relatively unscathed" (Collier, 2007). As a result Estonia has capitalized on the internet security market. They are called upon to assist during attacks and to speak to different business and IT groups on internet security issues. Estonian government leaders have spoken to allies, regional organizations and international organizations to improve IT security and cooperation. (Ibid.)

When Georgia's IT infrastructure was attacked in August 2008 specialists from Estonia's Computer Emergency Response Team (CERT) travelled to Georgia and assisted response efforts to counter the attacks (DPA, 2008). This example demonstrates how Estonia has established itself as a major player in an emerging field, as they are too small to make a large impact on the international scene through the use of economic or military power. Estonia has been able to establish itself as a major player in Europe and among NATO members as an expert in cyber security and cyber war. Their expertise has allowed them to lobby for increased IT awareness and for increased cooperation to defeat or deter future cyber attacks. (Nikiforov, 2008)

In 2003 Estonia proposed a cyber excellence centre in Tallinn even before it became a member of NATO. In light of Estonia's expertise in IT the NATO Cyber Defence Centre was approved. In May 2008 the centre opened in Tallinn with Estonia providing the leadership and personnel to man the centre. Estonia emerged as a leader within NATO and leads the effort to protect the IT structure of NATO. (Socor, 2008)

The continuous threat of cyber attacks against its IT structure, and the dedication of public officials to improve IT security resulted in a comprehensive national cyber security strategy. This strategy, developed by the Ministry of Defence, was adopted by the Estonian government in May of 2008, just over a year after the attack on its IT systems. The main measures of its strategy included IT security measures that strengthened their defensive posture, as well as developed their expertise and awareness in the IT field. Estonia now looks to strengthen the international legal framework to ensure that the IT system is protected by laws, and that violators of the law will be prosecuted. Estonia has also taken the charge of increasing international co-operation not just to protect their systems but to protect the global cyber system. (Estonian Ministry of Defence, 2008)

## 4. Cyber concerns for former Soviet satellites

What do the countries of Estonia, Georgia, Lithuania and Kyrgyzstan have in common? They are all former Soviet satellites and have all been allegedly cyber attacked by Russia.

### 4.1. Georgian cyber attack

On July 20th, 2008 the website of the Georgian president came under a denial of service cyber attack. The attack shut the website down for 24 hours and was a precursor to a larger cyber attack that would come less than a month later (Melikishvili, 2008/2009). On August 8th, 2008 a coordinated distributed denial of service attack was made against the Georgian government websites at the same time that Russian forces were engaged in combat with Georgian forces. As the ground attacks increased so did the cyber attacks. This was the first time that a cyber attack was done in conjunction with armed conflict. (Ibid)

The cyber war between Georgia and Russia focused on shaping public opinion on the internet. Georgian and Russian supporters used a variety of cyber techniques including distributed denial of service attacks and the creation of fake web sites to control how their version of the "truth" was delivered to the public. (Thomas, 2009:55-59)

Georgia's IT infrastructure was not very advanced so the disruption of service was not as complicated as it was in Estonia. Banking, media and government websites were blocked disrupting the flow of information throughout Georgia and to the outside world. The websites of the Ministry of Foreign Affairs and the National Bank were vandalized by adding pictures of the Georgian President and Adolf Hitler (Melikishvili, 2008/2009). The cyber attacks against Georgia were different from the cyber attacks on Estonia, as these attacks included distributed denial of services using botnets, but they also included SQL injection attacks that are harder to identify than a botnet attack because they require less computers than a botnet attack. The SQL injection attack shows a greater expertise in the ability to conduct a cyber attack than the cyber attacks on Estonia's IT infrastructure. (Secure Works Press Release, 2008)

Georgia received considerable assistance in countering the cyber attacks and in communicating internally and internationally. *Google* provided domain space to protect the websites of the Ministry of Foreign Affairs and *Civil.ge*, a Georgian Daily online news service. A private American internet service provider (the head of the company is an ethnic Georgian) assisted the Georgian government by hosting the Georgian President's website. The President of Poland also assisted the Georgian government by placing official press releases on his website. Estonia even sent two information security specialists from its Computer Emergency Response Team to assist Georgia in countering the cyber attacks. According to outside investigators there is no direct proof of any Russian government involvement in the cyber attacks. But what is undeniable is that even without proven Russian government involvement it remains clear that the Russian government benefited from the cyber attacks. (Melikishvili, 2008/2009)

### 4.2. Lithuanian cyber attack

Lithuania faced its own attacks in June 2008 three days after it passed a law outlawing the use of Soviet and communist symbols; over 300 websites were attacked. Some were denial of service attacks while other sites were vandalized with the Soviet hammer and sickle. Prior to the attacks and the passage of the law, Russian and Lithuanian ties had deteriorated because of Russia's refusal to compensate Lithuanian victims of Soviet labour camps, and Russia's leveraging of energy resources for political gain. Lithuania also blocked talks on an EU-Russia partnership. The animosities between the two countries have provided observers with a clear motive that the attacks were by the Russians. The reason for the cyber attacks against Lithuania was similar to the cyber attacks against Estonia, both attacks were in response to a government action that was unpopular to the Russian people. (McLaughlin, 2008)

### 4.3. Kyrgyzstan cyber attack

The latest country that has come under a cyber attack from computers in Russia is Kyrgyzstan. On January 18th, 2009 Kyrgyzstan's two main internet servers came under a denial of service attacks shutting down websites and email within the country. The originators of the attacks were traced back to Russia (Rhoads, 2009). The attacks occurred on the same day that the Russian government was pressuring Kyrgyzstan to stop U.S. access to the airbase at Bishkek at Manas. The airbase is a key logistics centre that supports the U.S. war efforts in Afghanistan. According to Don Jackson, a senior security researcher at *SecureWorks*[4], the distributed denial of service attacks are believed to be directed towards any opposition that is not in favour of the closure of the airbase. While it is unproven whether the government was behind the attacks the implication is that cyber attacks will be used against any opposition to the Russian government (Bradbury, 2009).

The cyber attacks on Georgia, Lithuania and Kyrgyzstan have two characteristics in common. The first characteristic is that the cyber attacks were initiated because of opposition to the Russian government and secondly that there is no proof that the Russian government was involved in the cyber attacks. Regardless of who is initiating the attack it is clear that opposition to the Russian government could result in a cyber attack which could disrupt critical government infrastructure.

## 5. Compelling realities for the North Atlantic Treaty Organization

Cyber defence is a critical issue for NATO. U.S. General James Mattis, NATO's Supreme Allied Commander for Transformation, articulates the importance of cyber defence for NATO by stating, "We cannot say that we are not going to defend the Web that everybody needs" (Tanner & Peach, 2008). Nations that are party to the North Atlantic Treaty agree on Article 5 "that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all…" (The North Atlantic Treaty, 1949). Does a cyber attack fit the requirement of an armed attack? A senior NATO official asked, "If a member state's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?" (The Economist, 2007). However, the current political reality is that they are not the same. Prior to the cyber attacks on Estonia, NATO's cyber strategy was focused on NATO's ability to protect its own IT infrastructure. Now, the current reality is, is that the NATO's strategy must focus on assisting allies as they protect their own IT infrastructure during an attack (North Atlantic Treaty Organization, undated a).

Members of NATO have taken several steps in defining a cyber strategy and implementing a cyber defence. As early as 2002, at the Prague Summit, cyber defence appeared on NATO's agenda. At the Prague Summit NATO leaders agreed to the implementation of a NATO Cyber Defence Program. The program consisted of a NATO Computer Incident Response Capability and for NATO to use the latest cyber defence measures (North Atlantic Treaty Organization, undated a). In the spring of 2006 cyber defence was made a priority for NATO during the Riga Summit. The issue of cyber security gained even more attention when Estonia, a NATO member, was cyber attacked in 2007 (EU News, Policy Positions & EU Actors online, 2008).

NATO conducted a thorough assessment of its IT structure and how it would defend itself against a cyber attack. This assessment led to an October 2007 report on cyber defence that was issued to the Allied Defence Ministers. The report recommended measures to improve protection against cyber attacks (North Atlantic Treaty Organization, undated a). What followed was a cyber defence policy in early 2008 and the creation of a NATO Centre of Excellence for cyber defence in May 2008 (North Atlantic Treaty Organization, 2008a). In April 2008, during the Bucharest Summit, cyber defence was part of the summit declaration. The declaration emphasizes the need to protect key information systems, the sharing of best practices, and for Allied nations to provide assistance to counter a cyber attack (North Atlantic Treaty Organization, 2008b).

Even though not all NATO nations are part of the Cyber Defence Centre the centre works to enhance the cyber defence capabilities of all NATO members. The centre itself is not even funded by NATO but by the nations that participate in the running of the centre of excellence. The centre has been charged with doctrine and concept development, awareness and training, research, development, analysis, and lessons learned. The experts at the centre also serve as cyber defence consultants for NATO members North Atlantic Treaty Organization, undated b).

The compelling reality for NATO is that cyber warfare has affected member nations and continuous to be a realistic threat for the organization and for its members. NATO members are continuing to develop ways to counter future threats by sharing best practice information, information on technical cyber defences, and by agreeing to assist member nations in countering a cyber attack.

## 6. Multilateral initiatives

Only a few international treaties on cyber security exist making international cooperation to prevent cyber attacks extremely difficult. Even finding and then holding accountable a person that commits a cyber crime is almost impossible without some international cooperation (Organization for Security and Co-Operation in Europe, 2008). In the aftermath of the cyber attacks on Estonia the European Union commissioned a study to examine the issues concerning cyber security facing members of the European Union. This section will examine the European Union study and other multinational initiatives that have an impact on the cyber security of former Soviet satellites and Russia. (Cornish, 2009)

### 6.1. Convention on Cybercrime

The Council of Europe has established a treaty on cyber crime that entered into force[5] in 2004. Twenty-two Council of Europe member nations, along with the United States, have ratified the treaty agreeing to international cooperation concerning cybercrime issues. The Russian Federation has not agreed to the treaty making it difficult for states to resolve issues with Russia concerning cyber crimes in an international forum (Council of Europe, undated a). This treaty is still significant because it is the first international treaty on crimes committed on the internet (Council of Europe, undated b).

The main goal of the convention, as stated in the preamble, is to protect nations against cybercrime, by adopting laws and regulations, and fostering co-operation internationally. The states that become a party to the Convention on Cybercrime agree to adopt laws that create criminal penalties for committing crimes on the internet. The convention outlines several areas that states have agreed to make criminal statutes on issues such as illegal access of computer systems, system and data interference, and other computer related fraud. Nations that are party to the convention also agree to cooperate with investigations, to provide mutual assistance concerning cyber crimes, and to pursue the collection of evidence. The extradition of alleged cybercriminals is also agreed to by parties to the treaty. Disagreements between states that have ratified the treaty include direct negotiations, settlement in front of the European Committee on Crime Problems (CDPC), a tribunal for arbitration or adjudication in front of the International Court of Justice. The Convention on Cybercrime gave a framework for cooperation among member states for the prosecution of cyber criminals by removing safe havens for the cyber criminals. (Council of Europe, 2001)

However, Russia does agree to the convention and it protects citizens who engage in cyber misconduct by preventing their extradition out of Russia. Failing to sign the convention agreement also prevents Russia from having any legal standing to prosecute trans-national cyber criminals who attack Russia's IT infrastructure.

### 6.2. Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe (OSCE) has a tradition of promoting the security and stability of Europe. This tradition of promoting security and stability since 2004 has included cyber security. The OSCE's initial focus on cyber security concerned the use of the internet for recruiting, fundraising, and communication by terrorist organizations. In 2006 the OSCE's efforts began to focus on protecting vital information infrastructures against cyber attacks. Debate in the OSCE has not led to great change but has been a forum for further cooperation in cyber security in Europe. In June 2008, the Estonian Defence Minister, Jaak Aaviksoo, in an address to members of the OSCE, said there is "an immense amount of work to be done [concerning cyber security]." Minister Aaviksoo used the forum of the OSCE to use his nation's experience in defending against cyber crime to increase international cooperation in Europe. This statement by the Estonian Defence Minister sums up OSCE's efforts concerning cyber defence, they are still in the talking phase and have at least recognized the importance of cyber defence (Cornish, 2009:20-21). The OSCE will continue to be a forum to publicize grievances for European nations that have had their IT infrastructures attacked by Russian hackers. European nations will judge Russia on its cooperation with the OSCE in finding and prosecuting individuals who engage in cyber attacks.

### 6.3. The European Union

Estonia continues to lobby for improved international cooperation in cyber security as it calls on the European Union (EU) to pass legislation concerning crimes committed on the internet. While addressing the

European Parliament, Toomas Hendrik, the Estonian President, called upon the EU to pass legislation that make cyber attacks against public and private web sites a criminal act (Jones, 2008). The EU has several initiatives involving different agencies but lacks an overall cyber security strategy. The European Commission has the Information Society and Media Directorate General, the European Network and Information Security Agency (ENISA), and the Contact Network of Spam Authorities that deal with different aspects of cyber security. The Information Society and Media Directorate has a program to improve the content of the internet by protecting people from child pornography, racism, and other harmful online content. The ENISA is an agency that was created in 2004 to raise awareness of cyber security issues and to promote best practices by member nations with the EU. The Contact Network of SPAM authorities is an initiative to counter SPAM and share information on best practices between EU member nations. (Cornish, 2009:24-27)

The European Parliament has established several standing committees concerned with cyber security issues. The Committee on Industry, Research, and Technology (ITRE) is concerned with establishing information technology networks within the EU. The Committee on Civil Liberties, Justice, and Home Affairs (LIBE) is responsible of the protection of personal information on the internet for members of the EU. The Committee on Foreign Affairs is responsible for the Security and Security policies of the EU which includes internet security policies. (Cornish, 2009:26)

The European Police Office (EUROPOL) is an agency of the Police and Judicial Co-operation (PJC) that has more of a direct role in EU cyber security in the context of combating terrorism, organized crime, and financial crime (Cornish, 2009:25). Although cyber security is addressed by the EU there is no organization within the EU to ensure that there are no contradictions in cyber security policy among all of the various EU agencies, commissions, and co-operations. The European Parliament commissioned a study on cyber security published February 2009 that examined security challenges concerning the internet for the EU. The study recommended that clear roles should be defined for cyber security responses with the many EU organizations, including the establishment of the post of cyber security coordinator and the establishment of a common operating vision for cyber security in order to achieve operational consistency across the EU (Cornish, 2009:31). The EU and Russia work together on different challenges including drug and human trafficking, organized crime, and counter-terrorism. Russia is also the EU's third largest trading partner (European Commission, 2009). The EU's cyber security organizations can offer a framework for increased cooperation to defeat cyber attacks that originate from or are directed at Russia.

### 6.4. The United Nations

The main purpose of the United Nations (UN) is to maintain international peace and security among the different nations of the world (United Nations, 1945). The focus for cyber security for the UN, through the UN Security Council, has been on countering terrorism. Debates among the UN General Assembly started in 2002 highlighted the growing dependence on IT use. Out of discussions came a warning that law enforcement activities would not be sufficient but that more efforts in cyber security need to be made on prevention. (Cornish, 2009:17)

The International Telecommunication Union (ITU) is the main organization that is responsible for cyber security within the UN framework. The ITU's goal is to enhance cyber security in order for individuals, businesses and nations to have confidence in the use of cyberspace. The ITU uses its Global Cyber Security Agenda, which began in 2007, to promote its goals of increased cyber security. The ITU has not been an agency for the enforcement of legislation and international agreements concerning cyber security but has focused on assisting in building nation's capabilities for cyber security (Cornish, 2009:17-18). Former Soviet satellites can cooperate with the ITU to improve their cyber defences against cyber criminals from Russia or any other nation. The UN will continue to be a forum for Russia to voice grievances or defend themselves against world opinion in matters involving international peace and security including cyber security.

### 6.5. Relevance of multilateral initiatives

Although the Russian government cooperates with Europe and other nations on a variety of economic and security issues, individuals, organizations, and governments are able to exploit the weaknesses of the international system in order to use the internet for criminal activities without fear of any major reprisals. Significant effort has been made towards cyber security since the cyber attack on Estonia in 2007, but much more needs to be done among national and international organizations to ensure genuine cyber security. The framework for increasing cyber security exists, but it will take the cooperation of many nations, including Russia, to make a difference in cyber security.

## 7. Implications for the United States

The cyber attack on Estonia should be considered a significant wake-up call for the United States. Even though the attacks had no direct impact on the U.S., Estonia is a NATO ally and the attack clearly showed aggressive intent seeking advantage. When the attacks occurred the U.S. sent experts to assist and help Estonia with its cyber defences. Jaak Aaviksoo, the Estonian Defence Minister, was told by U.S. officials that Estonia coped better than the U.S. is likely could in responding to a cyber attack. The Estonian Computer Emergency Response Team (CERT) was able to concentrate on protecting vital sites by coordinating government and public efforts. They were also able to create diversions which caused hackers to attack sites which were already disabled or not very important. (Collier, 2007)

The cyber attack on Estonia demonstrated the importance of legal obligations for the U.S. in rendering support to its allies during a cyber attack (Gee, 2008). The cyber attack also showed the vulnerability of an IT system, raising the question, if it could happen to Estonia could another trans-national cyber attack of this magnitude happen in the U.S. (Griggs, 2008)? The convention on cybercrime, which the U.S. is a party to, outlines principles for providing mutual assistance regarding cybercrime (Council of Europe, 2001). The convention does not mention cyber attacks or cyber war but treats such activities as crimes (Korns & Kastenberg, 2008/2009). Because only 23 countries have agreed to this treaty, its force in the international community is limited (Gee, 2008).

Several members of NATO are participating in the Cyber Defence Centre of Excellence that was established in Estonia, but the U.S. only agreed to the creation of the cyber defence centre as an observer. The cyber defence centre is working on issues of cyber security that affect NATO along with the U.S (The Associated Press, 2008). What will the U.S.'s response be if a cyber attack destroys infrastructure and kills citizens in an allied country, and then that ally declares war because of the attack? The plausibility of such an attack was demonstrated in 2007 when scientists from the Idaho

National Laboratory demonstrated how a cyber attack could cause a power plant to overload its system, begin to smoke, and then break down which caused physical damage to equipment. Currently, both international law and NATO's framework lack coherent responses that are legal in the event of such an attack. The cyber attackers could limit options for the U.S. under such a scenario by routing their cyber attack through countries which do not have laws or agreements to cooperate with the U.S. The cyber attacker could remain completely anonymous if the country where the attack was routed through refused to hand over information identifying the cyber attackers. (Gee, 2008)

Cyber attacks on the U.S. government IT infrastructure are not new. In March 1998 a cyber attack was launched against computer systems of the U.S. government, private universities and research labs computer systems that lasted for over three years. Government investigators named the attacks "Moonlight Maze." The cyber attacks targeted gaining access to sensitive but unclassified information (Abreu, 2001). John Adams, a National Security Agency (NSA) consultant says that government investigators have identified seven internet addresses involved in the cyber attacks that originated in Russia. Dion Stempfley, a former Pentagon computer analyst, believes that the U.S. prove that the Russian Federation government is sponsoring the attacks but there is evidence that they are allowing or otherwise permitting the cyber attacks. The cyber attacks which resulted in the theft of technical defence information were serious enough that the U.S. State Department issued a formal complaint to the Russian Federation. (Loeb, 2001)

In *Global Trends 2025*, a study conducted by the National Intelligence Council, states over the next two decades non-military aspects of warfare, including cyber, will be prominent (National Intelligence Council, 2008). According to Secure Works, a cyber security company, in 2008 over 20 million attacks originated from computers within the United States (Secure Works Press Release, 2008). In 2008 the U.S. Department of Homeland Security created the National Cybersecurity Centre to counter these threats (Griggs, 2008). The threats to the U.S. infrastructure and technology are moving at a much faster pace than the creation of government structures to counter the threat.

Even a casual observer can see that there is a cyber threat to the U.S., but how is that connected to any Russian involvement in cyber attacks? There are three recent examples of how cyber attacks, that may have allegedly originated in Russia, that demonstrate danger for U.S. and Russian relations. These examples show how attacks against an IT structure were used as cyber pressure to influence nations or organizations.

The first example is when Radio Free Europe's internet sites in April 2008 in Eastern Europe were shut down because of a denial of service attack. The attack lasted two days and coincided with the planned coverage of the anniversary of the 1986 Chernobyl disaster. The attacks effectively shut down the websites which stopped the flow of information from Radio Free Europe, a U.S. sponsored program (America.gov, 2008).

Another example is the malware (malware is a term used to identify illegal computer access including computer viruses) attack on U.S. Department of Defence computer systems in November 2008. According to *WMD Insights*[6] the computer attacks are thought to have originated from Russia. The attacks seemed to target military computer systems and affected the U.S. central command along with computers in Iraq and Afghanistan. The attacks led to a ban on the use of external computer flash drives on military computers throughout the world. (Melikishvili, 2008/2009)

The latest example of an attack that may have originated in Russia is the January 2009 denial of service attack that was directed at the government websites of the Republic of Kyrgyzstan. One theory on why the attack was started was because of Kyrgyzstan's support of the U.S. in its war on terror in Afghanistan. This shows the significance of a cyber attack not directed against the U.S. but against one of its allies. (Rhoads, 2009)

One senior fellow at the Centre for Strategic and International Studies in Washington, D.C. believes there is no adversary that can defeat the U.S. in cyber space. A spokesman for the U.S. Department of Homeland Security commented that the U.S. government is able to protect itself from cyber attacks, but the U.S. IT system is not completely impenetrable. The director of a non-profit research institute, the United States Cyber Consequences Unit, stated that because the U.S. controls so much internet bandwidth that most of the people that want to harm the U.S. lack the capabilities to shut down U.S. servers. (Griggs, 2008)

The U.S. faces a wide variety of challenges in protecting its own IT structure along with facing the reality of the challenges of its allies' cyber defences. In the future the U.S. may face cyber attacks that could cause the deaths of its or its allies' citizens due to the effects of a cyber attack on an electrical system. The U.S.'s bilateral agreements with countries that hold a strategic U.S. interest could be affected by the use of a cyber attack to influence leaders. The cyber threats to the U.S. are real and continued attention by the leaders must focus on this threat.

## 8. The weakest link – the computer user

As you read this article you could be an accomplice to a cyber criminal without even knowing that your computer is conducting a worldwide distributed denial of service attack. The actions or lack of action of computer users have contributed to the ability of hackers in Russia and elsewhere to conduct their attacks in relative anonymity.[7] The internet has vulnerabilities and the individual computer user contributes to the vulnerabilities of private and government IT systems.

In 1997 the National Security Agency (NSA) conducted an exercise to find out how vulnerable government IT systems were to external cyber attacks. They named the exercise "Eligible Receiver." Thirty-five IT specialists were given the mission to hack into government systems. They could use any software programs that were available on the internet and they were only given a few limitations. The IT specialists couldn't use any classified hacking software that belonged to the NSA and they could not violate U.S. law. The IT specialists were also confined to U.S. government computer systems. (Verton, 2003:32-33)

What they discovered was how easy it was to hack into government systems, into both classified and unclassified networks. With the free software that they downloaded from the internet, the NSA specialists were able to conduct distributed denial of service attacks, delete or modify sensitive information and shut down or reformat systems. Along with the software they used, personal contact methods were also used to gain access into the systems. The NSA computer specialists would use telephone calls or emails to gain passwords or entry into a system by posing as a supervisor or technician. The IT specialists were surprised at how easily government and military members delivered their passwords without question. Even though the exercise was conducted in 1997, and may seem dated, it gives us a great example of how a dedicated effort can disrupt any IT system. (Verton, 2003:32-33)

As noted earlier, external flash drives were banned from use with military computer systems. Authorized users unknowingly passed intrusive malware files from computer to computer infecting IT systems throughout the U.S. Central Command. The ban on flash drives complicated the sharing of information throughout the theatre. The malware file was even found on a classified network. This is one more example of how an individual can spread malicious software infecting multiple computer systems because of a lack of computer security protocols. (Melikishvili, 2008/2009)

One vulnerability that is associated with computer users is that some people who become hackers are former employees with a grievance against their former employer. Such people may be motivated by a personal grudge against the U.S. government because they were fired or lost their job due to a reorganization or downsizing. Their actions as hackers are usually malicious in nature as such people steal or corrupt data, deface websites, or shut down systems. (Conway, 2007:82)

Even more dangerous than an angry former employee is a case of cyber espionage. This is where an individual who is motivated by money or ideology sells highly sensitive IT security information. One such case involves Herman Simm and his wife, Heete Simm, from Estonia (Melikishvili, 2008/2009). Mr. Simm was arrested in September 2008 for allegedly passing highly classified information on cyber security and missile defence to members of the Russian foreign Intelligence Service (SVR). Mr. Simm was the head of the State Secret Protection Office where he was responsible for protecting Estonia's classified information. Mrs. Simm was a lawyer who was previously employed at the Estonian national police headquarters. Mr. Simm had access to classified information concerning NATO and allies of Estonia including the operational information of the NATO Cooperative Cyber Defence Centre based in Tallinn. If the Estonian government had access to a secret so did Mr. Simm. The amount of classified information that was compromised is unknown, but may be quite large. Mr. Simms allegedly became a Russian spy in the mid-1990's and was paid millions of dollars from the Russian Government. Regardless of how secure a country's IT structure is, it is still vulnerable because some people will compromise sensitive cyber security information for personal gain. (Melikishvili, 2008/2009)

Along with the vulnerabilities already mentioned there are always problems with software products. Some software is easy for hackers to take advantage of because of security deficiencies. Computers may be infected before the user or software company has identified the problem. Then it will take time for the software company to produce a security patch. It will take even more time to get the patch to the computer program user and for the security patch to be installed. During this time the infected computer program may have already infected other computers in a system or throughout the internet. (Wilson, 2006:15-16)

A major vulnerability for any IT system is the computer user. Whether the computer user is a military member, a government employee, or just a computer user sitting in front of his computer at home, their practices can cause serious damage to a computer system. Normal computer users receive little or no training in the best security practices. (Wilson, 2006:14)

The cost of poor security practices can be high. Along with the loss of data or the disruption of service there is also the physical cost associated with malware and viruses. For example, in 2007 the Federal Bureau of Investigation (FBI) uncovered a botnet campaign that caused losses of over 20 million dollars (Cornish, 2009:9). One of the botnet hackers that was caught by the FBI and sentenced to prison used botnets to steal peoples' identities and bank account information. After gaining access to personal information and passwords he made on-line purchases and transferred money from the bank accounts. Another cyber attacker used a phishing scheme where he collected information through infected emails (Wired Staff, 2009). This section highlighted how the computer user has made IT structures even more vulnerable and the Simm affair demonstrates how cyber espionage adds to that vulnerability. If countries like the U.S. and Estonia that have highly developed IT infrastructure can be attacked, it is not hard to imagine the vulnerabilities less developed former Soviet satellites have in their IT development phase.

## 9. The Russian Federation

In this article study several cyber attacks have been attributed to Russia. Regardless of whether the government of Russia is responsible for the attacks, or merely sanctioned them, for many the perception remains that Russia was behind the cyber attacks. I will examine Russia's use of cyber warfare against former Soviet satellite states. (Davis, 2009)

The Russian government views itself as the victim in the case of the cyber attacks on Estonia in 2007. According to sources in the Kremlin the website of the President of Russia came under a cyber attack. This was supposedly the largest attack the Russians have faced and it appeared that the servers used to originate the attack were located in the Baltic States. The Deputy Press Secretary of the Russian President, Dmitry Peskov, countered accusations from Estonia with the fact that Russian government websites are under attack every day from all over the world. (The Baltic Times, 2007a)

Even as cyber attacks occurred against Georgia, Russians said that they were also the victims of cyber attacks. *Russia Today*[8], a major media source in Russia, was shut down because of a denial of service attacks directed towards its websites. IT security specialists that work for *Russia Today* believe that the denial of service attacks originated from Tbilisi, the capital of Georgia. (Watson, 2008)

In the aftermath of the cyber attacks on Estonia, Georgia, and other attacks mentioned in this article, the Russian response was to deny any involvement in any cyber attack. When confronted with evidence that some of the attacks originated from Russian government computers members of the Russian government countered with the fact that computers from all over the world were hijacked and used to attack different computer systems. (The Baltic Times, 2007a)

Another fact that Russian officials are quick to point out is that the only person arrested for the 2007 cyber attacks on Estonia was an Estonian. Dmitri Galushkevich, a 20 year old ethnic Russian, who was convicted for the cyber attacks. Some members of the Estonian government have issued statements doubting the involvement of the Russian government in the cyber attacks. (Greenberg, 2008)

With the finger pointing that ensues after a cyber attack it is still unclear who was behind the attacks. The actions of cyber activist groups, or hactivists, will be examined in the case of the cyber attacks on Estonia and Georgia. Hactivists are individuals that use cyber attacks to take a patriotic or political stand on a political or international issue. (Melikishvili, 2008/2009)

During the protests in Estonia, increased chatter and postings on how to conduct and participate in denial of service attacks were found on Russian internet chat sites (Melikishvili, 2008/2009). Along with the denial of service attacks, some of the Estonian government websites were hacked in order to deface the site. The sayings on the websites were very pro Russian and very anti Estonian. Joshua Davis in *Wired Magazine* supports the view that the reason behind the attacks was nothing more than Russian pride. (Davis, 2009)

In March of 2009 a member of a Russian pro-Kremlin youth group, Konstantin Goloskokov, publicly took responsibility for creating the 2007 cyber attacks on Estonia. Goloskokov is a leader of the youth movement *Nashi* that has routinely conducted cyber attacks and intimidation campaigns on behalf of the Russian government. The government of the Russian Federation is able to maintain separation from the youth group because it does not directly fund their activities. The youth groups are funded by pro-government business owners who are trying to gain favour from the Russian government (Shachtman, 2009). Goloskokov believes that his actions were not illegal but were, "an act of civil disobedience organized within the confines of virtual space" (Buranov, Vodo & Yegikyan, 2009). The cultural aspects or belief that actions in the cyber world are beyond the law is a consequence for the Russian government and how cyber attacks affect their international relationships.

An assistant to Sergei Markov, a member of Russia's State Duma lower house, has also admitted to using his own initiative to conduct cyber attacks against Estonia (Baltic News Service, 2009). Rein Lang, the Estonian Justice Minister, is contemplating issuing a European arrest warrant for individuals who have admitted to taking part in the attack. The idea for the warrant is not to send law enforcement officials into Russia, but to have the alleged perpetrators arrested whenever they leave the country (Baltic News Service, 2009). Aleksandr Gostev, director of the Kaspersky Lab's Global Research and Analysis Team, explains that hackers who participate in a distributed denial of service attack violate the Russian Criminal Code (Article 274, *Violation of the Rules Governing the Use of Computers, Computer Systems, or Networks Thereof*) and can be imprisoned for four years for violating the code. But he also states that the article is rarely used (Buranov, Vodo & Yegikyan, 2009). The examples of Russian citizens admitting to participating in the Estonian cyber attacks are grounds for

Russian citizens to be arrested in other parts of Europe if Russia fails to uphold its own laws.

Similar actions occurred in the Georgian cyber attacks. Messages were posted on Russian hacker forums on how to participate in shutting down Georgian websites. The website StopGeorgia.ru was also established as a private forum to coordinate the denial of service attacks. Jeff Carr, a network security expert and cyber analyst, established an all volunteer group to investigate the cyber attacks. Throughout the course of the investigation, which they named *Project Grey Goose*, no evidence was found to implicate the Russian government. This was just another example of a hactivist movement which had the collective power to conduct a cyber attack against a government. (Melikishvili, 2008/2009)

The *Project Grey Goose* investigation has looked at hactivists and how they can independently conduct cyber attacks. It also focused on a criminal gang known as the *Russian Business Network* (R.B.N.). The R.B.N. is based in St. Petersburg and engages in criminal cyber activities. According to Don Jackson, the director of threat intelligence at Secure Works, some of the cyber attacks used against Georgian websites originated from computers under the control of the R.B.N. As is the case with any cyber attacks it is very difficult to establish who is completely responsible or if there is any Russian government sanctioned involvement. (Markoff, 2008a)

This article has already noted that there are other groups involved with cyber attacks against former Soviet satellites. The evidence of Russian government involvement will now be investigated (Davis, 2009). Indeed, some statements made by Russian government officials suggest Russian government involvement in cyber attacks. Prior to the cyber attacks in Estonia the Russian government protested the movement of the Russian memorial, the Bronze Soldier, to the Estonian government. The Russian government warned how disastrous the move would be to Estonia. What followed were the protests and the cyber attacks. (Davis, 2009)

The head of the Russian Army Centre for Military Forecast, Colonel Anatoly Tsyganok, made comments to the Russian news outlet, *Gazeta*, about the cyber attacks on Estonia. He believes that there was nothing wrong with the attacks because there are no international agreements established. Colonel Tsyganok also believes that NATO couldn't do anything to stop the attacks, and that they were highly successful. (prygi.blogspot.com[9], 2008)

The most telling example of Russian government involvement in cyber warfare was with Herman Simm selling IT secrets to the Russian Foreign Intelligence Service that was discussed earlier in this article. This examples shows that the government of the Russian Federation is actively seeking information on cyber defences and is willing to pay large sums of money (Mr. Simm is accused of selling cyber security secrets for millions of dollars) to receive information on cyber security. (Melikishvili, 2008/2009)

There are also cases where cyber attacks were used against people who are in opposition to the Russian government. One such example is with Gary Kasparov, Russian opposition party leader, had his website shut down for two weeks due to denial of service attacks during the Russian presidential campaign. John Palfrey, a researcher at Harvard Law School, believes that several organizations in Russia who plan to protest, or act in opposition to the Russian government, are subjected to cyber attacks in an attempt to control the information that is getting to the public. (Greenberg, 2008)

Another example of Russian government complicity is the lack of assistance or interest in tracking down those responsible for the cyber attacks against governments of former Soviet satellites (Davis, 2009). The evidence of government involvement remains circumstantial, but certain facts are clear concerning cyber security and former Soviet satellites. If there is opposition to Russian Federation policy than that country that is in opposition is likely to be subject to a cyber attack and it has been shown that the Russian Federation actively collects information on other countries cyber defences.

## 10. The future of Russian cyber warfare

The perception exists among different nations (some of those nations have been discussed earlier in this study) that the government of the Russian Federation has been involved in cyber attacks. This section will examine future trends concerning the use of cyber attacks by, or sanctioned by, the Russian Federation government. The cyber attacks against Estonia and Georgia have forced Russia to evaluate its future cyber strategy. In examining the Russian focus on improving its cyber strategy some conclusions can be drawn about the future of Russian cyber warfare. (Panarin, 2008)

As with many countries that have an advanced IT system, a sub-culture of hacking has developed. Even though the state sponsored university in St. Petersburg produces computer programmers that are highly regarded it is believed that most of the hackers are young and not educated at the university level. The reason behind the growth of Russian computer hackers is the prestige and monetary reward that hacking garners in a growing IT infrastructure. (Varoli, 2000)

The criminal organization, R.B.N., has been able to conduct its cyber activities with little interference from the Russian Federation government. The R.B.N. is very difficult to track on the internet as they are able to locate their activities from several different locations. The group has been involved in several different types of criminal cyber activities such as the use of malware, identity theft, and child pornography. Without any concerted effort to stop the R.B.N., and their ability to operate anywhere, R.B.N. is an organization that is positioned in Russian cyber activities now and in the future. (Markoff, 2008a)

One example of latitude and scope created by Russian indifference, a group identified by a computer security firm as a Russian gang conducted a botnet based computer operation operating in Wisconsin. The Russian gang was controlling as many as 100000 computers in an effort to steal passwords and information. As soon as the system was shut down the Russian gang moved its host computer system to a site in the Ukraine. This shows how resilient these gangs are when they can relocate their operating systems to countries that are out of reach of law enforcement of the country that they are targeting. (Markoff, 2008b)

The Russian responses to the recent cyber attacks are a guide to how they will react in the future. Valery Yashenko, vice director of the Institute of Information Security Issues at Lomonosov Moscow State University, advises the Russian government on the issues of cyber terrorism. Yashenko believes that there should be greater international cooperation concerning cyber security but does not think that the cyber attack on Estonia was of any real consequence. Yashenko indicates that the Russian Federation government is only concerned with cyber security matters that affect his own government. (Davis, 2009)

Not surprisingly, the Russian Federal Security Service (F.S.B.) is believed to employ its own hackers (Varoli, 2000). The manner of recruiting is a little different than normal ways of looking for employees. When an IT specialist or hacker is caught committing a cyber crime they may receive an offer to work for the F.S.B., or face criminal charges. According to a Russian computer security specialist hackers that were working for the F.S.B. attacked pro-Chechen web sites. According to the same computer security specialist the F.S.B. hackers have hacked into opposition newspapers in order to control information about the Russian Federation government and its leaders. The recruitment of hackers for offensive cyber attacks vice cyber defences is an indication of the future Russian Federation government cyber strategy. (Varoli, 2000)

The Russian Federation government has shown the capability for law enforcement in cyber space. Laws exist in Russia that make crimes committed on the internet punishable under the law. Russia has even established a computer crime unit, which it called Department "K," which operates under the Ministry of Internal Affairs of the Russian Federation (MVD). Department "K" is responsible for the detection, prevention, suppression, and solving crimes involving information technology. In 2008, Department "K" was able to identify 158 computer crimes and shut down seven illegal internet operations. The MVD is currently conducting Project "Clean Network" aimed a combating illegal uses of the internet (Ministry of Internal Affairs of the Russian Federation, undated). It remains to be seen whether the efforts of Department "K" will have any negative impact on the R.B.N. or the cyber gangs that support the Russian government.

The Russian Federation Public Chamber[10] organized a discussion on Russian information warfare in September 2008 and *Just Russia*[11] political party hosted an international conference on information warfare in October 2008. The conclusions of the meeting were that Russia has grossly underestimated the role of information warfare and failed to 'champion' their goals and interests in the world media. (Panarin, 2008)

Dr. Igor Panarin, the Dean of the Faculty of International Relations of the Ministry of Foreign Affairs Diplomatic Academy in Moscow, used the information warfare discussions to make several recommendations to the Russian government concerning information and cyber warfare. Dr.

Panarin proposes that Russia develop specialized management and analytical structures to counter information threats. Dr. Panarin proposes a system that has eight key components. (Panarin, 2008)

The first component is the creation of a Council for Public Diplomacy that will develop a single point of view for both the Russian government and Russian businesses. Government and business leaders are to be included on the council in order to ensure that all activities concerning foreign political media are coordinated. The second component is to create an advisor to the President of Russia for Information and Propaganda Activities in order to coordinate the foreign political information activities of the administration of the President, the government, different ministries, and the Russian Security Council. (Panarin, 2008)

The third and fourth components are to create state holding companies, one for foreign media affairs and one for the internet. The holding companies would be combined between business and government to see that Russian political positions were broadcast to the world. The information would not just be focused towards ethnic Russians but would be focused globally towards economic partners, future partners, adversaries, and overall world opinion. (Panarin, 2008)

The fifth component would be the creation of an information crisis action centre in order to ensure that Russia maintains the initiative when delivering the state message to the world. The information crisis action centre would be responsible for developing talking points and themes that would support the government in any crisis. (Panarin, 2008)

The sixth component would create an information countermeasures system that would counter enemy information operations. The information countermeasures system would include assets from business and the government. The seventh component focuses on a system on nongovernmental organizations that would operate throughout the world. (Panarin, 2008)

The final component would consist of a system for training information warfare specialists. This system would use existing educational institutions and academies to train specialists that would be able to operate at the diplomatic, management, or individual level. The training system would also include the creation of an Information Special Forces that are highly trained to for conducting information operations in a crisis. (Panarin, 2008)

Along with the creation of the information warfare system Dr. Panarin believes that financing for information warfare needs to be increased by both the Russian government and by Russian businesses. The increased attention on information warfare is designed to increase Russia's image throughout the world and ensure that Russia is prepared for future conflict in the cyber and information arenas. (Panarin, 2008)

Statements by Russian government officials have been very similar to Dr. Panarin's position which makes the future of cyber warfare in Russia offensively poised. Colonel Aleksandr Drobyshevskiy, head of the Russian Federation Ministry of Defence Directorate for Press Service and Information, stated that Georgia won the information war during the conflict in South Ossetia and there is a need for the development of information and telecommunications technologies within the Ministry of Defence. Colonel Drobyshevskiy further advocates the creation of an information warfare system. (Svobodnaya Pressa, 2009)

Another clue to the future of Russian cyber warfare is the development of a new information warfare defensive strategy by the Russian Armed Forces General Staff. Colonel-General Anatoliy Nogovitsyn, Deputy Chief of the General Staff, stated that leading world powers will be able to conduct full-scale information warfare and that Russia must be prepared (Usov, 2009). General Nogovitsyn believes that Russia will be involved in a large-scale information war within two to three years that will be fought in the cyber world (Litovkin, 2009).

The existence of hackers that support the Russian government and information specialists within the Russian government have created an asset that will be used during future cyber conflicts. The Russian government's emphasis on developing cyber strategies will enable Russia to be prepared for future cyber conflict.

## 11. Countermeasures

We need to examine what can be done to counter cyber crimes and protect a nation's IT structure. Cyber countermeasures can be taken at the international level, followed by cyber defences at the national level, and ending with actions that an individual computer user can make to improve cyber defence.

The International Telecommunication Union (ITU), the organization within the UN that is responsible for the international oversight of the world's telephone system, is developing a system for oversight of the internet. The ITU is working towards a convention against cybercrime that will provide international cooperation on issues concerning internet communications (Schrank, 2007). Members of the international community will need to work together in order to track and prosecute cyber criminals that operate outside of the country that is being attacked. Nations will also have to work together to share technical data to maintain cyber defences to keep up with the newest and ever changing cyber attacks. Hackers routinely share information on new techniques that can penetrate IT defence structures. Nations need to do the same to protect their own IT infrastructure, the same IT structure that affects the entire globe (Lipson, 2002:47-48).

Individual countries can improve their cyber defences within their own boundaries which would also improve the cyber security of the international IT system. Countries can make laws making cyber crimes illegal with punishments and programs that will deter potential cyber criminals. Governments can create a system that increases co-operation between the government, businesses, and academic institutions in order to improve their cyber defences. This co-operation could lead to an IT infrastructure that is resilient and able to withstand and recover from a cyber attack with little or no permanent damage to a country's IT structure. (Schrank, 2007)

In 8th section the computer user was identified as the weakest link in an IT system. Some individual countermeasures are easy to accomplish for any computer user. Actions like keeping antivirus and anti-spyware software up to date along with updating your web browser and operating system can greatly enhance your own computer security. Even following safe computer practices of not opening unknown attachments on emails that may carry viruses or malware are very instrumental in making the cyber environment more secure (Secure Works Press Release, 2008). The U.S. Department of Homeland Security (DHS) has tips for computer users posted on their website to increase internet security. The main points of the DHS website are to promote personal responsibility for increasing cyber security and to promote best practices for safe computer usage. The best practices that DHS advertises are to make cyber security a habit by following three core practices. The three core practices are to "install anti-virus and anti-spyware programs and keep them up to date, install a firewall and keep it properly configured, and to regularly install updates on your computer's operating system" (Homeland Security, 2008). Computer users are the first line of defence in cyber security and their actions can help protect the cyber infrastructure that is used by all.

## Conclusion

The international system is lacking in its ability to effectively manage issues of cyber security. The Russian Federation is perceived by the international community as a country that engages in or supports groups that are involved in cyber crime. International and regional organizations along with countries that interact with the Russian Federation have to deal with a reality that they may be the target of a cyber attack if they are in opposition to the government of the Russian Federation.

The issue of cyber security is ongoing. As more of the former Soviet satellites become more developed with an advanced IT structure they will have to face the realities of cyber attacks. Regardless of whether the government of the Russia Federation has been involved in any cyber attacks, or will be in the future, the reality remains that nations, groups, or individuals that are in opposition to Russia may face a cyber attack. The cyber attacks will be used to influence public opinion or to influence government leaders through the use of cyber pressure. Future conflicts that involve the use of force will also see cyber attacks in conjunction with combat operations. Currently international agreements and laws are inadequate which allows cyber attackers to take advantage of the lack of such laws and can conduct acts of civil disobedience on the internet.

The conflict in Georgia has been a motivator for military reform which includes reform in the cyber arena. The Russian government and the Russian military will continue to develop systems to improve both their offensive and defensive cyber capabilities. Russia will continue to capitalize on their diaspora present throughout the world to support their political positions but will have to realize that some of that diaspora will be in opposition to them and provide private support to organizations and nations that have received cyber attacks. Russia's active collection of cyber defence secrets will also be a combat multiplier for them in future conflicts either alone in the cyber world or as part of a ground conflict.

Organizations and nations will be best served by creating a resilient defence in depth while educating users and managers of IT systems in best practices to counter the threat of a cyber attack. This defence in depth includes technical responses to counter the threats while ensuring that their IT systems are resilient and become effective after an attack. President Bush remarked in 2001 that, "It's time to work together to address the new security threats that we all face. And those threats are not simply missiles or weapons of mass destruction in the hands of untrustworthy countries. Cyber-terrorism is a threat, and we need to work on that together" (Verton, 2003:248).

## References:

Aaviksoo, Jaak, 2007 (Nov. 28th). *Address by the Minister of Defence of the Republic of Estonia*, at The Centre for Strategic & International Studies, Washington, D.C.

Abdullaev, Nabi, 2006 (Oct 31st). New "Just Russia" Party Says Putin Knows Best. *St. Petersburg Times.* http://www.times.spb.ru/index.php?action_id=2&story_id=19303; (accessed April 10th, 2009).

Abreu, Elinor, 2001 (May 10th). Epic cyberattack reveals cracks in U.S. defense," (CNN.com, May 10, 2001) http://archives.cnn.com/2001/TECH/internet/05/10/3.year.cyberattack.idg/ (accessed April 10th, 2009).

Anon. 2007 (May 12th). A Cyber-Riot. *The Economist.* p. 55. http://lumen.cgsccarl.com/login?url= http://search.ebscohost.com/login.aspx?direct=true &db=a9h&AN=25048355&site=ehost-live; (accessed December 19th, 2008).

Baltic News Service, 2009 (March 12th). Estonian Minister Lang Says European Arrest Warrant Possible for Cyber Attackers. *Baltic News Service.* https://www.opensource.gov, Document ID EUP20090312010002; (assessed April 10th, 2009).

Bradbury, Danny, 2009 (Feb. 5th). The Fog of Cyberwar. *The Guardian.* http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-acess; (accessed March 22nd, 2009).

Buranov, Ivan; Vodo, Vladimir and Yegikyan, Seda. 2009 (March 12th). Pro-Kremlin Activist Admits Attack on Estonian Websites, Denies Criminal Wrongdoing, Translated by Open Source Centre. Moscow: *Konmersant Online.*

https://www.opensource.gov, Document ID CEP20090312021013; (accessed April 10th, 2009).

Central Intelligence Agency, page updated as of Dec. 4th, 2008. *The World Fact Book, Estonia.* https://www.cia.gov/library/publications/the-world-factbook/geos/ en.html; (accessed December 13th, 2008).

Collier, Mike, 2007 (Dec. 17th). Estonia: Cyber Superpower. *Business Week.* http://www.businessweek.com/globalbiz/ content/dec2007/gb20071217_535635.htm; (accessed August 27th, 2008).

Collier, Mike, 2007. Estonia: Cyber Superpower. *Business Week.* http://www.businessweek.com/ globalbiz/content/dec2007/gb20071217_535635. htm?chan=globalbiz_europe+index+page_top+stories. (accessed August 27th, 2008).

Conway, Maura, 2007. *Information Warfare: Separating Hype from Reality,* ed. Armistead, Leigh. Washington, D.C.: Potomac Books, Inc. p. 82.

Cornish, Paul, 2009 (Feb. 2nd). *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks.* Brussels: European Parliament. pp. 24-27. http://www.europarl.europa.eu/activities/committees/ studies.do?language=EN; (accessed February 19th, 2009).

Council of Europe, *Convention on Cybercrime* (Budapest, November 23rd, 2001) http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; (accessed February 19th, 2009).

Council of Europe, *Convention on Cybercrime, Chart of signatures and ratifications,* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=& DF=&CL=ENG; (accessed February 19th, 2009).

Council of Europe, *Convention on Cybercrime: Summary of the treaty,* http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm; (accessed February 19th, 2009).

Davis, Joshua, 2009. Hackers Take Down the Most Wired Country in Europe. *Wired Magazine*, Issue 15.

Davis, Joshua, 2009. Hackers Take Down the Most Wired Country in Europe. *Wired Magazine*. Issue 15.

DPA, 2008 (Aug. 11th). Estonia sends experts to Georgia to help combat cyber attacks. *The Earth Times.* http://www.earthtimes.org/articles/show/224942,Estonia-sends-experts-to-georgia-to-help-combat-cyber-attacks.html ; (accessed August 27th, 2008).

Estonian Ministry of Defence, 2008 (May). *Cyber Security Strategy.* Tallinn. p. 3.

EU News, Policy Positions & EU Actors online, 2008 (April 4th). NATO agrees common approach to cyber defence. *EurActiv.com.* http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377; (accessed February 18th, 2009).

European Commission. *External Relations: Russia.* http://ec.europa.eu/external_relations/russia/ index_en.htm (accessed April 8th, 2009).

From wire reports, 2007 (June 8th). Estonian PM, justice minister insist that cyber attacks came from Kremlin computers, *The Baltic Times.* http://www.baltictimes.com/news/articles/18038/; (accessed December 19th, 2008).

From wire reports, 2007 (May 18th). Kremlin denies involvement in cyber attacks on Estonia, *The Baltic Times.* http://www.baltictimes.com /news/articles/17908/; (accessed December 19th, 2008).

From wire reports, 2007 (May 18th). The Kremlin denies involvement in cyber attacks on Estonia. *The Baltic Times.* http://www.baltictimes.com /news/articles/17908/; (accessed December 19th, 2008).

Gee, Alastair, 2008 (Nov.). The Dark Art of Cyberwar. *Foreign Policy.* http://www.foreignpolicy.com/story/cms.php?story_id=4553; (accessed December 19th, 2008).

Greenberg, Andy, 2008 (May 14th). The State of Cyber Security: When Cyber Terrorism Becomes State Censorship. *Forbes.com.* http://www.forbes.com/2008/05/14/cyberattacks-terrorism-estonia-tech-security08-cx_ag_0514attacks.html; (accessed December 19th, 2008).

Griggs, Brandon, 2008 (Sept. 12th). U.S. at risk of cyberattacks, experts say. *CNN.com.* http://www.cnn.com/2008/TECH/08/18/cyber.warfare/index.html; (accessed Oct. 24th, 2008 and Feb. 14th, 2009).

Homeland Security. *Cybersecurity: Make it a Habit.* http://www.dhs.gov/zxprevprot/programs/ gc_1202746448575.shtm (accessed March 11th, 2009).

Jones, Huw, 2008 (March 12th). Estonia calls for EU law to combat cyber attacks. *Reuters.* http://www.reuters.com/articlePrint?articleId=USL 1164404620080312; (accessed February 19th, 2009).

Kampmark, Binoy, 2003 (Autumn). Cyber Warfare Between Estonia and Russia. *Contemporary Review.* pp. 288-293.

Korns, Stephen and Kastenberg, Joshua, 2008/2009 (Winter). Georgia's Left Hook. *Parameters.* Vol. XXXVIII, No. 4. p. 64.

Lipson, Howard, 2002. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.* Pittsburgh, PA. pp. 47-48.

Litovkin, Dmitriy, 2009 (Feb. 27th). The General Staff is Preparing for a Cyber War, Translated by Open Source Centre. Moscow: *Izvestiya.* https://www.opensource.gov, Document ID CEP20090302358005; (accessed March 7th, 2009).

Loeb, Vernon, 2001 (May 7th). Pentagon Computers Under Assault. *Washington Post.* A02.

Markoff, John, 2008a (Aug. 13th). Before The Gunfire, Cyberattacks. *New York Times*. A1.

Markoff, John, 2008b (Aug. 6th). Russian Gang Hijacking PCs in Vast Scheme. *New York Times*. C6.

McLaughlin, Daniel, 2008 (July 2nd). Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites. *Irish Times*. p. 10. http://lumen.cgsccarl.com/login?url=http://proquest.umi.com/pqdweb?did=1503762091&sid=2&Fmt=3&clientld=5094&RQT=309&VName=PQD; (accessed February 20th, 2009).

Melikishvili, Alexander, 2008 (Dec.)/2009 (Jan.). Recent Events Suggest Cyber Warfare Can Become New Threat. *WMD Insights*. http://www.wmdinsights.com/I29/I29_G3_RecentEvents.htm; (accessed February 19-20th, 2009).

Ministry of Internal Affairs of the Russian Federation, undated. *Clean Network*, Translated by Open Source Centre. Moscow: Ministry of Internal affairs of the Russian Federation. https://www.opensource.gov, Document ID CEP20090406546003 (accessed April 9th, 2009).

National Intelligence Council, 2008 (Nov.). *Global Trends 2025: A Transformed World.* U.S. Government Printing Office. p. 71. http://www.dni.gov/nic/NIC_2025_project.html; (accessed February 20th, 2009).

Nikiforov, IIya, 2008 (Sept. 29th). Hot Fellows in Saakashvili's Service. Tallinn Exports Specialists in Intelligence and Democracy. Trans. Open Source Centre. *Moscow Nezavisimaya Gazeta.* https://www.opensource.gov, Document ID CEP20080929021009; (accessed December 18th, 2008).

North Atlantic Treaty Organization, 1949 (April). *The North Atlantic Treaty.* Washington D.C. http://www.nato.int/docu/basictxt/treaty.htm; (accessed February 17th, 2009).

North Atlantic Treaty Organization, 2008 (April 3rd). *Bucharest Summit Declaration.* Item 47. http://www.nato.int/docu/pr/2008/p08-049e.html (accessed February 18th, 2009).

North Atlantic Treaty Organization, 2008 (May 14th). NATO opens new centre of excellence on cyber defence. *NATO News*. http://www.nato.int/docu/update/2008/05-may/e0514a.html; (accessed February 18th, 2009).

North Atlantic Treaty Organization, undated. *Defending against cyber attacks*. NATO Topics. http://www.nato.int/issues/cyber_defence/ practice.html; (accessed February 18th, 2009).

North Atlantic Treaty Organization. Official website of the Cooperative Cyber Defence Centre of Excellence. http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD; (accessed February 18th, 2009).

Organization for Security and Co-Operation in Europe, 2008 (June 4th). *OSCE can play important role in cyber security, says Estonian Defence Minister* [on-line press release] http://www.osce.org/ pc/item_1_31483.html; (accessed February 19th, 2009).

Panarin, Igor, 2008 (Oct. 15th). The Information Warfare System: The Mechanism for Foreign Propaganda Requires Renewal, Translated by Open Source Centre. Moscow: *Voyenno-Promyshlennyy Kuryer*. https://www.opensource.gov, Document ID CEP20081016548020; (accessed October 22nd, 2008).

Prygi.blogspot.com, 2008 (Feb. 8th). *Ivan vs. Jaan. Russian Army Analyst to the World: You are defenceless against a cyber attack*. http://prygi.blogspot.com/; (accessed December 20th, 2008).

Rhoads, Christopher, 2009. Kyrgyzstan Knocked Offline. *Wall Street Journal*. p. 10.

Schrank, Peter, 2007 (May 24th). Cyberwarfare: Newly nasty. *Economist.com.* http://www.economist.com/ world/international/PrinterFriendly.cfm?story_id=9228757; (accessed August 8th, 2008).

Secure Works Press Release, 2008 (Sept. 22nd). *Compromised US and Chinese Computers Launch Greatest Number of Cyber Attacks, according to SecureWorks' Data.* http://www.secureworks.com/media/ press_releases/20080922-attacks/; (accessed February 19th, 2009).

Shachtman, Noah, 2009 (March 11th). Kremlin Kids: We Launched the Estonian Cyber War. *Wired Magazine*. Blog. http://blog.wired.com/defence/2009/03/pro-kremlin-gro.html (accessed March 14th, 2009).

Socor, Vladimir, 2008 (May 15th). NATO Creates Cyber Defence Centre In Estonia. *Eurasia Daily Monitor*. http://www.jamestown.org/single/ ?no_cache=1&tx_ttnews[tt_news]=33636; (accessed December 18th, 2008).

Statement by Ambassador of the U.S. Mission to the OSCE, Julie Finley, 2008 (May 8th). *Statement on Cyber-attacks Against Radio Free Europe in Belarus: OSCE will defend information-sharing efforts from criminal attacks, says Finley [transcript on-line]*. Vienna. http://www.america.gov/st/texttrans-english/2008/May /20080508115033eaifas0.3709833.html; (accessed February 20th, 2009).

Svobodnaya Pressa, 2009 (March 17th). *Ministry of Defence Planning Information Warfare*, Translated by Open Source Centre. Moscow: Svobodnaya Pressa. https://www.opensource.gov, Document ID CEP20090318358009; (accessed April 5th, 2009).

Tanner, Jari and Peach, Gary. 2008 (May 14th). NATO allies sign agreement on cyber defense centre. *International Herald Tribune*. www.iht.com/articles/ap/2008/05/14/europe/EU-GEN-NATO-Cyber-Defences.php; (accessed February 24th, 2009).

The Associated Press, 2008 (May 14th). NATO allies sign agreement on cyber defense centre. *International Herald Tribune*. http://www.iht.com

/articles/ap/2008/05/14/europe/EU-GEN-NATO-Cyber-Defences.php; (accessed February 24th, 2009).

The Russian Federation Public Chamber Website, undated. *About the House: On the Public Chamber of Russian Federation.* http://translate.google.ru/translate?hl=en&langpair=ru|en&u=http://www.oprf.ru/, (accessed April 10th, 2009).

Thomas, Timothy, 2009. The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia. *Journal of Slavic Military Studies.* pp. 55-59.

United Nations, 1945 (June 26th). *Charter of the United Nations*: Article 1. San Francisco. http://www.un.org/aboutun/charter/chapter1.shtml; (accessed February 19th, 2009).

Usov, Dmitriy, 2009 (Feb. 25th). Russia is Preparing for the Wars of the Future, Translated by Open Source Centre. Moscow: *Vzglyad.* https://www.opensource.gov, Document ID CEP2090227358005; (accessed March 7th, 2009).

Varoli, John, 2000 (June 29th). In Bleak Russia, a Young Man's thoughts turn to Hacking. *The New York Times* on the web. http://www.ssl .stu.neva.ru/psw/misc/29hack.html; (accessed December 20th, 2008).

Verton, Dan, 2003. *Black Ice: The Invisible Threat of Cyber-Terrorism.* Emeryville, CA: McGraw-Hill/Osborne. 32-33; 248.

Vesilind, Priit, 2008. *The Singing Revolution.* Tallinn: Varrak Publishers Ltd. p. 15, 78, 172.

Watson, Steve, 2008 (Aug. 12th). *Russia Today* Website Targeted In Cyber Attacks. *Infopass.net.* http://www.inforwars.net/articles/august 2008/120808Attacked.htm; (accessed December 19th, 2008).

Wilson, Clay, 2006. *Cyberterrorism and Computer Attacks*, ed. Brown, Lawrence. New York: Novinka Books. pp. 15-16.

Wired Staff, 2009 (March 5th). Botnet Hacker Gets Four Years. *Wired Magazine.* http://blog.wired.com/27bstroke6/2009/03/botnet-hacker-g.html; (accessed March 24th, 2009).

[1] Personal recollection of the author who lived in Estonia from July 2007 to June 2008.

[2] Multiple sources were used along with the author's personal recollections of living in Estonia. Three of the main sources that describe the attack are: Davis, Joshua, 2009. Hackers Take Down the Most Wired Country in Europe. *Wired Magazine.* Issue 15; Kampmark, Binoy, Autumn 2003. Cyber Warfare Between Estonia And Russia. *Contemporary Review.* pp. 288-293; Aaviksoo, Jaak, 2007 (Nov. 28th) Address by the Minister of Defence of the Republic of Estonia at The Centre for Strategic & International Studies, Washington, D.C.

[3] This reference offers an Estonian view of its history and underlines the reasons behind the friction between Russia and Estonia.

[4] SecureWorks is an internet security firm based out of Atlanta. The company tracks suspicious activities throughout the internet.

[5] Entered into force refers to the date that the treaty becomes enforceable according to the provisions of the treaty by the members that have agreed to the treaty.

[6] *WMD Insights* is a journal sponsored by the U.S. Defence Threat Reduction Agency.

[7] Idea based on comments used by Jaak Aaviksoo in 2007. Minister Aaviksoo used this technique to show that some members of the audience may unknowingly be helping cyber-terrorists. Jaak Aaviksoo, Address by the Minister of Defence of the Republic of Estonia delivered to the Centre for Strategic & International Studies, Washington, D.C., November 28, 2007.

[8] *Russia Today* is a globally broadcast news channel broadcast in the English language and owned by the Russian government news agency RIA-Novosti. Similar in programming to CNN and BBC but with a Russian perspective on events in the world news.

[9] Information from a Russian and English language blog that discusses issues concerning Russia.

[10] The Russian Federation Public Chamber is an organization created in 2005 to oversee all aspects of government and to act as a consultant to the heads of the Russian government. The Russian Federation Public Chamber Website, About the House: On the Public Chamber of Russian Federation, http://translate.google.ru/translate?hl=en&langpair=ru|en&u=http://www.oprf.ru/. (accessed April 10th, 2009).

[11] A Just Russia is a Russian political party created as an opposition party but still supports the power of the Russian executive branch (Abdullaev, 2006).