**Ideas That Shape (ITS)**

# Cyberspace: The Future Battlefields and Wars

NATO's Approach to Cyber Security and Cyber Defence: Can agency-centric organizational self-interest create weak links within a collective Cyber Security framework?


Author

Joseph Lerner



3rd Edition, August 24, 2012


**Edited by**

Dr. Terry Tucker (PhD), Daniel R. Little (PhD Candidate), Stephen Cheney

**Contributors**

**Dr. Michael Rainsborough (PhD),** Professor of Strategic Theory, Department of War Studies, King's College, University of London (UK)

**David Stone, (MA and MSc),** (Fmr.) British Military and Special Ops Technician, Maritime Security Consultant and Geopolitical Analyst

**Walter M. Bullock Jr. (MPA),** Major (ret.) USAF, USAF Air University: Command and Staff College, Computer Science, Hardware and Software Engineering

**Dan R. Little (PhD Candidate),** (Fmr.) Head of NATO Planning at the Warrior Preparation Center, US Forces-Europe; Researcher and Analyst, Diplomacy and Defence, Virginia Polytechnic Institute and State University (US)

**Dr. Terry Tucker (PhD),** Professor of History, Senior Analyst at the US Department of Defense (DoD), Senior Consultant at Spatial Terra Consulting Group (U.S.))

**Willem Smeets,** Diplomat (ret.) and former Senior Political Adviser to the Commander of NATO Headquarters. Lecturer: Diplomacy and International Organizations, The Hague University (Netherlands)

## Ideas That Shape (ITS)

Ideas that Shape (ITS) is a nonpartisan and autonomous Think Tank that has been active since April 2010. Ideas That Shape (ITS) is committed to serve as a medium and portal for exchange of ideas, knowledge and information that their areas of focus are Geopolitical and Sociopolitical Studies, International Relations, International Trade, Cultural Studies, Global Energy Security Analysis and International Security Studies.

Mailing address:

Website: www.ideasthatshape.com
E-mail: inquiry@ideasthatshape.com

**About the author:**

Joseph Lerner is an analyst whose areas of focus are Geopolitics and Cultural Studies. He has received his education in political science at Glendon College / Collège universitaire Glendon at York University. Joseph's academic interest is in investigating and learning about the logical thinking processes, methodologies and mechanisms by which the analysts, scholars and experts arrive to their conclusions. He currently serves on the panel of the Advisory Board of Ideas That Shape (ITS), and is a member of the Advisory Board of the Centre for Strategic Cyberspace + Security Science (CSCSS). In the past, Joseph has served on the Advisory Board of the Research Institute for European and American Studies (RIEAS).

***Editor's Note:*** *please be advised that the sources used in this paper are OSINT. Ideas That Shape (ITS) hopes that this paper would encourage further constructive academic and expert studies, discussions and debates about the highlighted issues.*

 

## Advisory Board

**Dr. Michael Rainsborough (PhD),** Professor of Strategic Theory, Department of War Studies, King's College, University of London (U.K.)

**Col. Gordon Forbes (ret.) (MA in International Relations),** York University; NATO Defense College; (Fmr.) Canada's Defence Attaché to Spain, Italy, Greece, Algeria and Morocco; (Fmr.) SSO National Security Studies and Deputy Director of Air Studies at Canadian Forces Command and Staff College (Canada)

**Dr. Mark Kass (PhD),** Doctoral Dissertation Chair at University of Phoenix, Member of Council on Foreign Relations, expert contributor to Huffington Post (U.S.)

**Willem Smeets (MA in International Relations),** Diplomat (ret.) and former Senior Political Advisor to the Commander of NATO Headquarters Naples, Italy; Lecturer: Diplomacy and International Organizations at The Hague University (Netherlands)

**Joseph Curry (Lt. res.),** Canadian Forces Intelligence Branch, Operation ATHENA, Afghanistan; Team Lead at Scotiabank Global Security Operations Centre. Recipient of Queen Elizabeth II Diamond Jubilee Medal (Canada)

**Dr. Terry Tucker (PhD),** Professor of History, Senior Analyst at the US Department of Defense (DoD), Senior Consultant at Spatial Terra Consulting Group (U.S.)

**Dr. Mark Fernando (PhD, Dip Psych, CPD & Associate, Oxford),** BSc. Hons (LSE), CME (Harvard), CPD and Fellow (Kent), Expert Adviser in Health and Public Health for International and National Health Organizations and Governments (Canterbury, U.K.)

**Clare Lopez (MA in International Relations),** Senior Fellow at the Center for Security Policy, Clarion Project and Gatestone Institute; Vice President of the Intelligence Summit; (Fmr.) Operations Officer with the Central Intelligence Agency (CIA); (Fmr.) Professor at the Centre for Counterintelligence and Security Studies; (Fmr.) Executive Director of the Iran Policy Committee from 2005-2006; 2011 Lincoln Fellow at the Claremont Institute (U.S.)

**Sergei Oudman (MA in International Relations)** American Military University, Political Consultant, International Relations, International Law, Conflict Resolution and Security Analyst (Brussels, Belgium)

**Ralf R. Zielonka, Lt. Col. (res),** German Forces (Bundeswehr), Freelance Security Consultant, Risk Assessment, Risk Analysis and Risk Management (Germany)

 

**Dr. Eve Sariyiannidou (PhD),** Researcher: EU Law and Policy at University of Bristol (U.K.); (Frm.) Official Observer at WEU Interparliamentary European Security and Defence Assembly and Government Defence Integrity (Oxford, U.K.)

**David Stone (MA and MSc),** (Fmr.) British Military and Special Ops Technician, Maritime Security Consultant and Geopolitical Analyst (GR)

**Dr. Milorad Krneta (PhD),** (Fmr.) Professor at London School of Economics and Political Science (LSE), Research and Analysis: Econometrics and Statistical Inference in Sociology (Canada)

**Capt. Nico Voorbach,** President of European Cockpit Association (ECA), Piloting Safety (Brussels, Belgium)

**Chuck Brooks (MA in International Relations),** Vice President, Client Executive for the US Department of Homeland Security (DHS) at Xerox, (Fmr.) Director of Legislative Affairs at the US Department of Homeland Security (DHS), (Fmr.) Adjunct Faculty at Johns Hopkins University (U.S.)

**Dr. Sven M. Spengemann (Jur. Sci),** Harvard Law School, visiting Professor at Glendon School of International and Public Affairs; Political and Constitutional Advisor served with the United Nations in Iraq, (Canada)

**Dr. Marc Gartenberg (PhD, ABD),** Chief Operating Officer / Chair – Cyber Warfare Centre at The Centre for Strategic Cyberspace + Security Science / CSCSS, Information Security and Defense Research (London, U.K., Washington, DC, Middle East), (Fmr.) Diplomat, Director of Global IT Training, US Department of State. (U.S.)

**Brian J. Patterson (CFE),** President and CEO at Ontario Safety League, Recipient of Queen Elizabeth II Diamond Jubilee Medal (Canada)

**Richard Zaluski (MSc),** President and CEO at The Centre for Strategic Cyberspace + Security Science / CSCSS, Information Security and Defense Research (London, U.K.)

**Dr. John M. Nomikos (PhD),** Director of Research Institute for European and American Studies (RIEAS), (Athens, Greece)

**Dr. Ioannis Galatas, B.Gen. (ret),** MD, CBRNe, Hellenic National Defence General Staff, Head of the Department of Asymmetric Threats at the Intelligence Analysis Branch of Joint Military Intelligence Division (Athens, Greece)

 

**Ioannis Chapsos (PhD Candidate),** Capt (ret.) Hellenic Navy, Researcher at Centre for Peace and Reconciliation Studies, Coventry University (Coventry, U.K.)

**Joseph Lerner,** Cultural Studies and Geopolitical Analyst (Canada); member of Advisory Board at The Centre for Strategic Cyberspace + Security Science / CSCSS (London, U.K.); (Fmr.) Senior Analyst and member of Advisory Board at RIEAS (Greece)

 

# Cyberspace: The Future Battlefields and Wars

After the Cyber-attacks that have targeted the Lockheed Martin, Google, Sony, Nintendo's database, the US Government and Military Websites and Canadian Government's Websites the reality of how the modern wars are fought has changed.

> *US Government and Military Websites Redirected to Chinese Servers: The report says telecommunications companies in China disrupted the Internet for only about 18 minutes — but they were a big 18 minutes. They "hijacked" about 15 percent of the world's online traffic, affecting NASA, the U.S. Senate, the four branches of the military and the office of the Secretary of Defense." Jason Ryan, ABC News, Technology, Washington, Nov. 17, 2010, link: http://abcn.ws/9XWRbm*

The time frame of the *Cyber-attack* that is indicated in this report was about 18 minutes. The speed of identifying and responding to any *Cyber Threat* is often within seconds or minutes.

The Chinese philosopher Sun Tzu admonished readers to first *'know themselves'* and second *'know the enemy'*. The raison d'être for founding the NATO alliance in the first place was to structure itself based on who the enemy was. NATO members knew who the enemy was, where they came from and what they looked like. Although the formation of a credible deterrence was a central theme, these equations are no longer valid in *Cyber-warfare*. The enemies are more often unknown. The attacks now possess the advantage of surprise: neither seeing, hearing, sensing or knowing when and where the enemy crossed the boundaries of sovereignty.

Worse still, the strategies, tactics and methods, not to mention the *Cyber-assault* patterns of behaviour tend to constantly change. All these elements require exploring Cyber-warfare's new uncharted territories; temporal geographies within an unseen Ethernet – today's *'no-man's land'*. Regardless, these must be meticulously studied and learned in greater detail. To protect information, it is imperative to decentralize and compartmentalize the information. Sensitive information should be kept on servers that are *NOT* connected to any network. A Cyber Security expert admonishes:

> *"**Cyber Threats:** there are NO Cyber Threats. All threats in the CYBER world have root/beginning with humans - their ability to access and control electrons. Cyber Threats are the realization of individuals' actions through the manipulation of electrons and the data they*

 

*represent." Walter M. Bullock Jr. (MPA), Major (ret.) USAF, USAF Air University: Command and Staff College, Computer Science, Hardware and Software Engineering*

In the past, the wars and battles were fought in the air, and on the ground, mountains, deserts; seas and oceans. This has changed. In the past, the enemy, and where the enemy came from and how the enemy looked like were known. When engaged in any combat mission NATO nations were able to physically identify and see the enemy. These equations no longer are valid in Cyber-Warfare.

> *"Thieves, voyeurs, spies and other nations regularly invade the electronic borders which surround our homes, businesses and government institutions. But because the job of safeguarding these borders falls between the twin public duties of securing economic progress and protecting national security, governments around the world can't decide which ministry to put in charge of internet security.*
>
> *What they ought to recognise, however, is that Internet Service Providers (ISPs) – and more broadly the whole communications sector – are the front line of cyber-defence, and should therefore shoulder more of the responsibility this entails."Melissa Hathaway, President of Global Strategies LLC, "Internet Service Providers are the front line of cyber-defence" Spring 2012, Europe's World, Spring 2012, link: http://bit.ly/T4Oem9*

Often, by the time that an intrusion or *Cyber-attack* is identified the damage is already done. In these cases, all that could be done are:

*a) contain the damage; and*

*b) prevent it from spreading to a wider area*

In such circumstances, NATO nations no longer are in a position to take their time and reflect on various thoughts and strategies, then develop countermeasures. This is a fact: the *Cyber-attack* has already been taken place. In such circumstances, often the only rational and pragmatic strategy is: to develop *New Multidimensional and Multilayered Cyber Security, Cyber Defence and Cyber Offence Strategies, Tactics and Systems.*

**New Cyber Security and Cyber Defence Strategies:**

> *"Along with the rest of the U.S. government, the Department of Defense (DoD) depends on cyberspace to function. It is difficult to overstate this reliance; DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and*

*control of the full spectrum of military operations." Department of Defense Strategy for Operating in Cyberspace, print July 2011, link: http://1.usa.gov/rkg46T*

According to the US Department of Defence Strategy for Operating in Cyberspace, the US cannot afford any form of Cyber Defence vulnerability by any possible means. Therefore, it will not be surprising to witness future battles fought behind computer monitors and *Cyber-operatives'* laptops.

*"The modern tools of technology speed more than information sharing; they speed the entire communications and data process, and contribute to a governments and commanders ability to apply decisive action. Cyberspace and the cyber domain is where information and intelligence is stored, shared and used for decision making.*

*The storage of this information mitigates the amplifying effect of intuition and risk when one feels that they have complete situational awareness - both, internally and externally. Taken together it gives one the sense of mitigating the seriousness of friction in decision making and speed to process constitute the ability to achieve and exert dominance and decisive action.*

*Cyber threats and security breach's compromise this ability, eliminate it, create doubts, increase risk, and cause decision making to stop; pending an assessment of what the security breach actually accomplished.*

*A key premise of training and training decision making in leadership, is to develop, hone, and imbue instincts to adapt to the 'Operational Level of War.'*

*Risk assessments and decision making about acceptable risk, include decisions about trust, information, capability and surprise, and the ability to rapidly process information and data to be "more" adaptable than your opponent when things go awry - in essence, the raw adaptability to friction and the operational level of war.*

*Although there is much open access in the cyber-domain, most, if not all governments, and the military, operate under the de-facto assumption that their system is 'closed.' A cyber breach now becomes an event that is just short of a "black swan" event.*

*The surprise and discovery of the breach becomes a "paralyzing" event that imposes a forced - either forced external or forced internal immediate stop to all activity. Imagine the psychological damage this inflicts when you rely extensively on this domain.*

*Think of your fear when you realized that your accounts have been hacked and your computer crashed and you are unsure of when the last 'back-up' occurred." Dr. Terry Tucker (PhD), Published by Spatial Terra Consulting Group, 2012.*

The future War Rooms in NATO's Command Centres will possibly look much different and highly advanced than today's. A considerable portion of the NATO's battle tactics and strategies are going to be developed by the Generals and Commanding Officers who are highly gifted computer scientists and Cyber Security Strategists and experts. Future *multilayered* and *multidimensional* battles and wars will be fought on the land, sea, sky, streets, deserts, mountains and in *Cyberspace*. If Sir

Winston Churchill was alive today he would have said, *"…….we shall fight our enemies on the seas and oceans, we shall fight with growing confidence and growing strength in the Air…. and we shall fight them in* ***Cyberspace****… We shall never surrender……."*

**Risk Assessment:**

> *"Cyberwar declared as China hunts for the West's intelligence secrets. Urgent warnings have been circulated throughout NATO and the European Union for secret intelligence material to be protected from a recent surge in cyberwar attacks originating in China. The attacks have also hit government and military institutions in the United States, where analysts said that the West had no effective response and that EU systems were especially vulnerable because most cyber security efforts were left to member states." The Sunday Times March 2010, link:* http://bit.ly/af3Qa1

It is unknown how much intelligence the Chinese hackers have acquired through recent Cyber-attacks. The extent of the loss of intelligence remains unknown. This makes the whole issue much more complex since there is not much to work with, when it comes to threat assessment and developing countermeasures. Further complicating our understanding is that no admissions by the authorities will ever be released to the public.

Nonetheless, NATO has to start upgrading its Cyber Security Systems, implementing new security measures and new Cyber Command Centres in order for NATO Forces to thwart the hackers.

What NATO shall be alarmed is the adversaries' ability to place NATO's Armed Forces and the NATO nations' national critical infrastructure in danger. For these reasons, one of the NATO's priorities MUST be: coming up with a coherent and extraordinary Cyber Defence Structure and Cyber Defence Strategies that includes simultaneously applying a *multilayered* and *multidimensional* strategic, tactical and technological countermeasures that are necessary to prevent NATO's combat and peacekeeping missions from being jeopardized.

 

The damage after each Cyber-attack taking place includes the astronomical costs of repairing, upgrading, redeveloping and restructuring NATO nations' computers, servers and Cyber Security Systems in light of these challenging economic time. McAfee in its 2009 Threat Analysis states *"The Threat Is Real":*

> *"Critical infrastructure owners and operators report that their networks and control systems are under repeated cyberattack, often from high-level adversaries like foreign nation-states. Assaults run the gamut from massive DDOS attacks designed to shut down systems all the way to stealthy efforts to enter networks undetected." Stewart Baker, CSIS; partner, Steptoe & Johnson, In the Crossfire, Critical Infrastructure in the Age of Cyber War, A global report on the threats facing key industries, McAfee Print 2009, link:* http://linkd.in/nkpzDM

**What Experts Say:**

It is imperative to realize that NATO nations undoubtedly need to focus on developing extraordinary and formidable *Cyber Defence Structures*, plans, strategies, tactics and technology to protect their entire critical infrastructures such as power plants, power-grids, telecommunication networks, financial institutions, military infrastructure, governments' databases, etc. However, what is much more needed is recruiting the gifted individuals who could develop and maintain all of what is mentioned. If any intruder could possibly bypass any NATO nation's Cyber Security Systems, hack into any of its key infrastructures, then the consequences could be devastating.

> *"If NATO wants to acquire that talent then they must go out and look for it! The students themselves do not see themselves as being something special until they are asked to meet so an so from such and such company, that has usually been informed by the Professors of the respective students aptitude in that type of field. Lateral thinking and problem solving are one of many signs that the Professors look out for as many of them are 'Head Hunters' for various companies, and often could make a small fortune if the student is 'hired'." David Stone, (MA and MSc), (Fmr.) British Military and Special Ops Technician, Maritime Security Consultant and Geopolitical Analyst*

Each time that a new technology is introduced and new techniques are developed, the NATO nations' invisible *Cyber Adversaries* get smarter and learn how to develop countermeasures and bypass the system. For this reason, the NATO nations' Cyber Security and Cyber Defence experts require to constantly and consistently study and keep themselves up to date. The science and art of Cyber Security and Cyber Defence are constantly changing and growing areas of focus. Furthermore, the cost estimation for the portion of the National Defence budget that is required to be dedicated to recruiting talented computer scientists and experts, and upgrading and maintaining the NATO nations' Cyber

 

Security and Cyber Defence Technology, are challenging tasks.

Addendum, it is imperative to realize and acknowledge that to eliminate the *Cyber Threats* and win the *Cyber Battles,* NATO nations' need to take the ability of the adversaries away, including the adversaries' ability to technologically mutate in timely fashion and learn about anything that relates to the NATO nations' Cyber Security and Cyber Defence technology and strategies.

Simultaneously, NATO nations, within the context of Cyber Security and Cyber Defence and as part of their strategies, shall aim to take away their adversaries' ability to have *cyber-resilience*. Furthermore, it is essential to realized that in *Cyber Warfare* nobody could hardly win in an absolute sense. *Cyber-war* is an ongoing war, with many battles won and lost on all sides, but the war will hardly end.

> *"The demand for new cyber personnel is high, commensurate with the severity of cyber threats. DoD must make itself competitive if it is to attract technically skilled personnel to join government service for the long-term. To achieve its objectives, DoD will focus on the establishment of dynamic programs to attract talent early, and the Department will leverage the 2010 Presidential Initiative to improve federal recruitment and hiring processes." Department of Defense Strategy for Operating in Cyberspace, print July 2011, link:* http://1.usa.gov/rkg46T

Even if NATO nations reach a point that they could confidently say that NATO's Cyber Defence Systems' hardware technology is good enough, then NATO nations still remain under threat, unless they consistently and constantly recruit highly talented computer scientists, Cyber Security and Cyber Defence professionals and experts. Probably this is why Joseph Stalin in the past stated: *"human resources decide everything"*. For these reasons, NATO needs to being to focus on recruiting highly gifted computer scientists, innovators, Cyber Security and Cyber Defence experts, who are able to immediately identify each single possible irregularity and threat through their ingenuity; then spontaneously develop countermeasures for it, both in terms of defence and offence as deterrents.

**NATO Nations and New Partnerships in Cyber Security and Cyber Defence:**

> *"Indian authorities have accused Pakistan of sponsoring a cyber attack against India, causing the panicked exodus of thousands of ethnic minorities from southern India last week. More than 35,000 people working and studying in southern and western Indian cities jammed train stations for about a week as they tried to flee in response to text-message warnings said to be from Indian Muslims angered at recent ethnic clashes in the northeast." Taha Siddiqui, India says Pakistan incited cyber attack that prompted thousands to flee, The Christian Science Monitor, Aug 24, 2012, link:* http://bit.ly/NRAvtk

The modern world of Cyber Security, Cyber Warfare and Cyber Defence require a total shift of paradigm. The old ways of strategic thinking no longer apply to our modern times. The kinds of Cyber-attacks that take place in our time, a decade ago, only existed in the science fiction books, TV series and movies. Regardless of what country or entity benefits from Cyber-intrusions or Cyber-attacks, they could be initiated from anywhere in the world. This calls for new alliances and NATO partnerships when it comes to developing and establishing the NATO nations' new Cyber Security Systems, Cyber Warfare Technology, Cyber Defence Strategies, and Cyberspace regulations. This MUST be done in a way that fully resonates with the NATO nations' democratic values, civil liberties and Freedom of Communications.

> *"With terrorists increasingly resorting to hacking and using internet for communications, India and the US Tuesday inked an agreement to promote increased collaboration in cyber security. The memorandum of understanding on cyber security was signed by R. Chandrashekhar, secretary, India Department of Information Technology, and Jane Holl Lute, deputy secretary for the US Department of Homeland Security (DHS). The agreement entails closer cooperation and the timely exchange of information on cyber security." India, US ink an agreement on cyber security, The Economic Times, July 2011, link:* http://bit.ly/nQvWEu

The agreement between the US and India that focuses on promoting increased collaboration in Cyber Security is probably one of the most important recent events, when it comes to international relations and defence collaboration. This is because of the following facts:

i*) India is a democracy that respects Human Rights and free-market*

*ii) India is a member of the Commonwealth of Nations*

*iii) Considerable population of India is fluent in English*

*iv) India suffers from the same terrorist threats as NATO countries do*

*v) India produces some of the most gifted computer scientists and Cyberspace experts*

*vi) India benefits from highly complex infrastructure that is already fibre-optic ready*

*vii) India is China's neighbour and is second to only China in population*

*viii) India has an important geostrategic position in the region. Map: http://goo.gl/a2lv7*

> *"The advantages about the participation of India mentioned are basically right. However, I wouldn't put all our eggs in one basket. In spite of its recent economic successes, India continues to face the challenges of poverty, illiteracy, corruption, malnutrition and inadequate public healthcare. All of these are potential breeding grounds for unrest or rebellion." Willem*

*Smeets, Diplomat (ret.) and former Senior Political Adviser to the Commander of NATO Headquarters Naples, Italy. Diplomacy and International Organizations, The Hague University (Netherlands)*

India is the future rising economic power in the region that shares the democratic values that are similar to that of NATO nations'. Although these elements make India one of NATO's closest friends in the region, and one of the best candidates for partnership in the NATO nations' war on terror, but according to the experts India is also one of the most geostrategically vulnerable countries in the region, as it faces threats from neighbouring Pakistan, as well as China's growing geopolitical role in the region.

*"NATO has the potential of establishing a credible Cybercommand. If you were to look at the Greek island of Crete for example, NATO has a significant presence on the island already in regards to Naval vessels, Air Force Logistics and Air Defense training.*

*Coincidentally, the European Union established ENISA (the European Network and Security Agency) on Crete as well.*

*For reasons that only Brussels could explain, the European Police Agency (EUROPOL) is establishing their European Police Cybercrime HQ at The Hague instead of bolstering ENISA.*

*Granted The Hague also hosts the NATO Consultation, Command and Control Agency (NC3A) and the future NATO Communications and Information Agency (NCI) but this poses a dilemma in terms of tactics and strategy.*

*ENISA is already functional. Co-locating a NATO Flag Command with ENISA is therefore quicker and cheaper.*

*Whatever future plans lie in store for Europe's most expensive real estate, the damage may already be done now.*

*Worse yet, The Hague is the only place in the cybersecurity world where everything: policy, vigilance and defense will be co-located. This not only puts the 'cyber cross-hairs' on EU, EUROPOL and NATO but regional commerce as well.*

*With that said the largest vulnerability may not be through 'the cloud' at all but people on the ground disrupting the proximate power sources." Dan R. Little (PhD Candidate), former Head of NATO Planning at the Warrior Preparation Center, US Forces-Europe; Researcher and Analyst, Diplomacy and Defence, Virginia Polytechnic Institute and State University (US)*

**Key to Success in Preventing and Defusing the Future Cyber-attacks**

1. *The NATO nations' ability to have an extraordinary Cyber Security and Cyber Defence Technology, and Cyber Defence Strategy in place; and*
2. *Recruiting gifted Cyber Security and Cyber Defence professionals and experts, who each possess an acute sense of Cyber Strategic Thinking, so that they could spontaneously identify*

*the threats, intrusions and their sources, then creatively improvise and contain them, and launch the proper offensive counter-attacks that could bring down the intruders' and abusers' systems.*

By following the above two-fold strategy, not only NATO nations could benefit from having a great state of the art Cyber Security and Cyber Defence Technology, but also NATO nations would have the solid Cyber Security, Cyber Defence and Cyber Warfare Strategies as deterrent in place. For these reasons, NATO nations need to adopt a new paradigm when it comes to developing their Cyber Security and Cyber Defence strategies and policies, as well as when it comes to who to allocate funds for the NATO nations' Cyber Security and Cyber Defence industries.

The cost of Cyber Security and Cyber Defence technologies and maintaining them is extremely high. The reason for this is: these industries always depend on highly gifted experts and professionals.

These are the industries that have created a *brain-drain* in the world, and will continue to do so in the future. Therefore, the common methods of dedicating a fixed annual budget for Cyber Security and Cyber Defence industries are no longer pragmatic.

NATO nations need to have a new creative financial system and policies in place, so that as new threats and challenges occur they could be spontaneously addressed and defused. This requires the ability to immediately and properly allocate funds to respond to these often unpredictable *Cyber Threats* and challenges. Furthermore, it is extremely essential to realize that allocating funds to cover the costs of the NATO nations', Cyber Security and Cyber Defence Strategies and Technology, are undoubtedly one of the most important priorities to focus on, when it comes to protecting the NATO nations' economy and interests in the world.

This research paperer has presented some of the issues that analysts, policy makers and defence experts deal with everyday. It is necessary to realize and acknowledge that NATO nations require a shift of paradigm, when it comes to how they look at their Cyber Security and Cyber Defence strategies, so that NATO nations could properly and successfully address these issues through accumulative knowledge and collaboration.

 

## Works Cited

United States Department of Defense Strategy for Operating in Cyberspace, July 2011, link: http://1.usa.gov/rkg46T

Stewart Baker, CSIS; partner, Steptoe & Johnson, In the Crossfire, Critical Infrastructure in the Age of Cyber War, A global report on the threats facing key industries, McAfee, 2009, link: http://linkd.in/nkpzDM

Jason Ryan, ABC News, Technology, Washington, Nov. 17, 2010, link: http://abcn.ws/9XWRbm

The Sunday Times March 2010, link: http://bit.ly/af3Qa1

Melissa Hathaway, President of Global Strategies LLC, "Internet Service Providers are the front line of cyber-defence" Spring 2012, Europe's World, Spring 2012, link: http://bit.ly/T4Oem9

Taha Siddiqui, India says Pakistan incited cyber attack that prompted thousands to flee, The Christian Science Monitor, Aug 24, 2012, link: http://bit.ly/NRAvtk

India, US ink an agreement on cyber security, The Economic Times, July 2011, link: http://bit.ly/nQvWEu

**Sources:**

i) http://www.enisa.europa.eu

ii) https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417

iii) http://www.ncia.nato.int/Pages/default.aspx

NB - The first edition of this research paper "Cyberspace: The Future Battlefields and Wars", written by Joseph Lerner, was published by Research Institute for European and American Studies (RIEAS) on August 21st, 2011, the second edition was published by EIA on December 29th, 2011. This newly revised and updated edition is published by Ideas That Shape (ITS) on August 24th, 2012.

 