**John G. Grimes**

**First National Congress on Security and Defense**

**For National Security Strategy**

**Lisbon, Portugal**

**24 June 2010**

# "National Infrastructure Critical to National Security"

## Introduction

I wish to thank the National Congress on Security and Defense and AFCEA's President of Portugal Chapter, CARLO RODOLFO, for the invitation to address the issues of national security strategy. I know that you all are waiting to eat, so my remarks will be brief.

## Bottom Line Up Front

Cyberspace, the newest of the borderless global commons, is lacking formal consensual behavioral norms. This fact challenges nations, states and the international community for a formal governance body to protect the sovereignty and territorial integrity of nations and global infrastructures. The national security strategies and policies of nations must address these factors.

**National Security Strategy**

I was asked to talk on the subject of Homeland Security and Defense, which is now a major topic area in most countries due to the terror attacks over recent years, and the **increased threat of attacks aided by technology** such as **1) THE INTERNET, 2) HIGH SPEED FIBER OPTIC SYSTEMS AND SATELLITE TRANSMISSIONS AND TV AND RADIO BROADCAST NETWORKS, AND 3) THE GLOBAL PERVASIVENESS OF COMPUTER TOOLS AND APPLICATIONS.** There is a **common thread that runs** through **national infrastructures** such as telecommunications and information systems networks, electric power grids, financial systems, government operations and air traffic control. All these national infrastructures are based on internet protocol technology. I will talk more about this later as part of cyber security vulnerabilities.

In today's conference sessions there were discussions on national infrastructure roles which are important in development of a national security strategy. I should mention that just last month President Obama submitted the US National Security Strategy required by the US Congress. I would like to quote two focus areas from the US Strategy that are **apropos** to this conference:

1. **Enhanced Security at Home** – "Security at home relies on our shared efforts to prevent and deter attacks by identifying and interdicting threats, denying hostile actors the ability to operate within our borders, protecting the nation's critical infrastructure and key resources, and securing cyberspace."

2. **Secure Cyberspace** – "Cyber security represents one of the most serious national security, public safety and economic challenges we face as a nation." "The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states. Defending against these threats to our security, prosperity and personal privacy requires networks that are secure, trustworthy and resilient. Our digital infrastructure, therefore, is a strategic national asset, and protecting it – while safeguarding privacy and civil liberties – is **a national security priority**."

**Real World**

In 2007, Estonia, a NATO member, was cut off from the internet by cyber attackers who besieged the country's bandwidth with a devastating denial of service attack. As we've heard numerous times from the Estonian Minister of Defense, the set of botnet attacks, which were probably launched by a bunch of hackers, disabled the websites of essential elements of the government and private sector such as banks, newspapers and the parliament, **threatening economic disruption** of the nation. The source of the attack was unclear, physical harm did not occur and Estonia never invoked NATO Article 5. This kind of attack raises issues such as the abilities of NATO and individual nations to make NATO Article 5 and critical policy and operational decisions at NET SPEED to prevent devastating infrastructure damage.

Three years ago this August, the nation of Georgia was under cyber attack by hackers prior to Russian troop movement into that country. President Shakashvilli's website was hacked and leading banks and

newspapers were taken down – one must ask, “is this a precursor to future warfare?”

Last year, US Government and military web sites came under attack around the time of the US Independence Day, 4 July, 2009. These attacks, which appeared to come from North Korea, were in fact botnets that originated from the UK. The attacks occurred at a time when diplomacy failed on nuclear issues between the two nations – Was this an act of war under the UN Charter?

Social networking sites such as Twitter, which have played a growing role in political protest movements around the world, have come under distributed denial of service attacks numerous times.

These are only a few samples of the cyber attacks on nation states, corporations and the public using the internet. When you look at it in the context of cost to governments, businesses and the public, it is mind boggling. A study presented by McAfee at the World Economics Forum in Davos-Klosters, Switzerland shows that global companies may have lost over $1 trillion worth of intellectual property to data theft in 2008.

## The Impact

It is estimated that it costs companies $55 billion to clean up the damages caused by attacks from computer worms and viruses such as “I Love You”, “SQL Slammer and SASSER.” These events are only the tip of the iceberg of cyber attacks that take place every moment of everyday in cyberspace. Cyber attacks can cause irreparable and unrecoverable damage to people’s lives and nations’ economies.

**Cyberspace environment**

Cyberspace is like a wild jungle. Nations and international bodies have been unable to establish and enforce the rules of the road for hackers, state actors and non-state actors, including criminals and terrorists. Some say that the cyberspace domain is not recognized as a global common, as are space and the high seas. I disagree. The internet is a global media; it can flow freely in cyberspace across most borders and territories with little or no international agreements or regulations. Where there are national laws or regulations, they do not extend to other nation's sovereignty and territories. The US Senate (Congress) had drafted legislation that requires the US State Department to work for international cooperation in the international community.

There are a number of international organizations and bodies that are addressing cyberspace/internet technologies, laws, cultures/ethics and policy. Dr. Tom Wingfield of the US has developed an excellent framework for international cyber security that that puts into context what he calls "The Cube". The Cube focuses on law, technology and policy. However, this algorithm does not go far enough; it must take in to consideration cultures or ethics which are different among regions and nations and which, in many cases, are based on religion and tribal norms.

It is clear that we need closer cooperation between government, industry, and academia to tackle the range of threats in cyberspace, both within nations and across borders. This cooperation must be local, regional and international. I believe that this conference is an important step in that effort. It is bringing together world-class talent from across all three sectors

to see how we can leverage our respective expertise. We are also learning about the unique challenges that different regions face, and the lessons that can be shared from our attempts to deal with those challenges.

The speakers and sessions that you will hear tomorrow will touch on a number of national security strategy issues, including the cyber security landscape, information sharing, standards, and international collaboration.

**SUMMARY**

It is very difficult to determine the attributions of cyber attacks on the global borderless digital networks and infrastructures that provide internet service to governments, commercial and the public. Everyone, including criminals and terrorists, is dependent upon the **global commons**.

Unless we get cyber crime under control, it will mutate into a very real national security issue with potentially catastrophic ramifications to our national infrastructures and homeland security.

Thank you very much. Please enjoy your dinner.