

WELCOME,
David
Sign Out
Edit Account

MY HOME

ALERTS

SEARCHES
0 Saved

REPORTS
1

CLIPBOARD

WHAT'S NEW

HELP
1-877-498-2537

Cyber Threat Warrants International Agency to Police: Commentary

ADD TO CLIPBOARD ADD TO REPORT E-MAIL PAGE PRINT PAGE

Commentary by Mati Kochavi and Clark Kent Ervin | August 12, 2011 12:00AM ET

(Bloomberg) -- Fifty-four years ago world nations ratified the creation of the International Atomic Energy Agency, which has played an indispensable role in maintaining global security, from the darkest days of the Cold War to the modern risk of atomic terrorism. Today we need a new international agency to deal with cyber war, a threat that, much like nuclear weapons, has the capacity to destroy infrastructure and incite chaos on an unimaginable scale.

Across the world, there are two billion Internet users and more than five billion mobile phone connections. Every day nearly 300 billion e-mails and five billion text messages are sent. This week, the use of Twitter and BlackBerry's messaging service enabled Britons to quickly mobilize for several nights of rioting and looting in London, showing how individuals with unprecedented tools and connectivity can orchestrate mass disorder and violence.

Some might question comparing the perils of the atomic age to those of the digital age. After all, the images of mushroom clouds and horrific death and destruction in Nagasaki and Hiroshima are forever seared in our collective consciousness. We have not yet experienced the true potential devastation of cyber war.

Every aspect of our modern lives -- from banking to transportation to national defense --- is reliant on cyber space. Every inch of public and private infrastructure in the developed world is digital, networked and thus vulnerable.

Cyber Attacks

We've seen this repeatedly in recent months. Attackers have breached the digital defenses of the CIA, NATO, the International Monetary Fund and the South Korean Foreign Ministry. Earlier this year, two Canadian finance ministries, the Treasury Board and the Department of Finance, fell victim to a cyber attack that took their offices offline for almost two months. The networks of Google Inc., the IMF, Citigroup Inc., Sony Corp., and oil and gas multinationals have all been infiltrated as well.

Cyber crime costs corporations and government organizations billions of dollars each year. An August 2011 research report conducted by the Ponemon Institute suggests that the median annualized cost of cyber crime incurred by large organizations was \$5.9 million per year. And the overall cost to the U.K. economy is \$44 billion a year, according to the first joint Government and industry report on this issue.

BGOV Briefing:

- [Internet-Service Provider Cybersecurity Practices: Private or Public Standards? \(pdf\)](#)

Additional BGOV Coverage:

- [Hackers Make Intellectual Property a Top Prize](#)
- [Data-Breach Notification Bill Approved by U.S. House Panel](#)

The threat goes far beyond the piracy of information, the theft of funds, and the cost of cleanup. Cyber war can -- and will -- have physical manifestations.

Threat to Society

It's no stretch to say that a concerted attack could have the very real potential to rend the fabric of our society --from the

corporations that employ us, to the governments that protect us, to the hospitals that care for us, and the utilities that keep the lights on and the water running.

Imagine the economic shock alone of a coordinated cyber attack on international financial institutions. Imagine consumers not having access to their cash or credit. Business would be unable to sell their products and services, or pay their employees.

Even this disastrous scenario pales in comparison with the potential destruction and loss of life in cyber war. It wouldn't require a great deal of time or skill for hackers to launch a coordinated attack on a nation's hospitals, for instance -- cutting off life support systems, scrambling blood bank records, darkening operating room, and ultimately taking lives.

No One Immune

Today, no corporation, government, or individual is immune from such attacks. And more to the point, there is little stopping those who wish to wage cyber war from doing so, thanks to the low barrier of entry for malicious cyber activity. Deploying even one nuclear weapon requires massive resources, years of development and vast technical expertise. Launching a cyber attack requires a computer, an Internet connection and modest programming skills.

And yet, our rapidly growing global dependence on cyber space stands in stark contrast to the adequacy of our cybersecurity. Despite what's at stake, the international response hasn't nearly equaled the seriousness of the cyber threat we face.

The imminent danger of cyber war requires coordinated, global action. Because cyber attackers see bytes not borders, code not countries, our defenses can't be limited by geography. Business leaders around the world and heads of state of industrialized nations must come together to protect life, liberty and property against this threat.

International Effort

The international community can best secure global peace in the 21st century with the help of a new agency, like the IAEA, that would investigate and deter cyber attacks.

A half-century ago, despite their fierce geopolitical rivalry, the Soviet Union and the U.S. realized that their collective

ABOUT THE AUTHORS



Mati Kochavi is the founder and chief executive officer of AGT International, a high-tech public safety and security firm.



Clark Kent Ervin was the first inspector general of the U.S. Department of Homeland Security and currently serves as director of the Aspen Institute's Homeland Security Program.

MORE FROM BGOV

[Dodd-Frank Divides Economists One Year Later: BGOV Debate](#)

[Bayer Seen Gaining From Block on Contraceptive Co-Pays: Insight](#)

[FAA Agreement Allows Cuts to Subsidized Flights: BGOV Analyst](#)

[How Do We Get Out of This Mess?: Commentary by Joe Minarik](#)

[India to Top U.S. Ex-Im Lending With \\$575 Million in Solar Deals](#)

future hinged on international cooperation to prevent an atomic calamity. Through their cooperation the IAEA was born.

Today, even adversarial nations must understand that the lack of international body dedicated to the prevention of cyber war means we are all at risk. International cooperation and coordination is needed once more to address a global, existential challenge.

“If the people of the world are to conduct an intelligent search for peace, they must be armed with the significant facts of today’s existence.” Those are the words of President Dwight David Eisenhower to the UN General Assembly in his famous Atoms for Peace speech, in which he first proposed the IAEA.

In 2011, the facts of existence are simple: our digital lives -- and our actual lives -- are at risk of being destroyed by cyber war. The international community must build a common defense before it's too late.

(Mati Kochavi is the founder and chief executive officer of AGT International, a high-tech public safety and security firm. Clark Kent Ervin was the first inspector general of the U.S. Department of Homeland Security and currently serves as director of the Aspen Institute’s Homeland Security Program. The views expressed are their own.)

To contact the authors of this column: Mati Kochavi at mkochavi@agt-news.com Clark Ervin at clark.ervin@aspensint.org

To contact the editor responsible: David Rapp at drapp5@bloomberg.net