Secure Infrastructures Through Renewable Energies

Erik Buschardt

Webster University

Fall 2015

Abstract

Cyberterrorism or cyberwarfare is widespread and prevalent in today's digital battleground, as is demonstrated via the STUXNET worm of 2009-10, [ZETTER 65]. As that is becoming increasingly certain, so is the need to eliminate ourselves of geopolitical ties that bind the outsourcing of energy and related infrastructure needs to certain foreign interests. These investments have become entangled in political discussions, and where these discussions fail to become resolved, hostile conflicts can result. Therefore, this paper will attempt to explain in various examples why it is important and critical to continue to invest in renewable technologies, in order to reduce our cyberterrorist exposures and vulnerabilities. Doing so will create an independence on finite fuel sources such as coal and crude oil, and will also provide a more healthy long term solution for our global ecosystem and biosphere, while eliminating a major national security threat facing our country today.

I. Topics of Conversation and Research - An Introduction

This paper aims to present to the reader a comprehensive summary of the current state of events regarding cybersecurity initiatives with specific regard to successful implementations of green energy technologies and how those technologies will secure the United States against a variety geopolitical cyberterrorist threats originating both from home and from abroad. Most evident is our reliance upon crude oil reserves drilled and exported from Middle Eastern countries, and the economic jitters felt by Wall Street generated by commodity shortages due to conflicts originating via traditionally kinetic warfare. As the 2016 presidential election draws near, this paper also illustrates the widening political gap as presented by the Democratic and Republican parties, what bills have been introduced, and what each platform aims to achieve. We supplement that with recent events taking place in Paris during the 2015 United Nations Climate Change Conference, (colloquially known as COP 21 or CMP 11).

Global warming will also play a part in recent discussions regarding oil reserves becoming newly available due to the lowering of drilling costs associated with the Arctic Ocean. Denmark (via Greenland), the United States (via Alaska), Canada and Russia are major stakeholders in this area, with competing territorial claims (Walsh 13). We also disprove three major misconceptions regarding moving forward with a ecologically sound agenda in order to enhance and protect our share of natural and renewable resources.

Federal actions taken to enhance our ecological "green" posture include the multiplication of renewable sources in order to retain an independence on foreign sources of fuel and energy, as mentioned by President Obama at recent climate talks in Paris. A recent Twitter announcement or "tweet" by @POTUS put it thusly: "We have multiplied wind power threefold, and solar power more than 20-fold" —@POTUS #ParisClimateConference #COP21

As far as the military is concerned, they have continued their mission towards an independence from adjoining civilian power grids in times of emergency. A recent article from Scientific American (Maron, 15) states that the military wants to make sure that when the power goes down, bases can stay online with backup energy sources called Smart Power Infrastructure Demonstration for Energy Reliability and Security, or SPIDERS). These so-called "micro-grids" would be enhance cybersecurity for each base by being completely independent from the commercial grid.

Military bases make an ideal test bed location for infrastructure development work because of the concentration of civil activities that parallel that of a small town. Ecological micro-grids also serve a dual purpose in that while it is not the primary mission of the Department of Defense to develop infrastructure for civilian use, but eventually technologies developed in battlefield do evolve into products made for civilian

life. Also, "bring green" also would save lives, as terrorists do target fuel convoys in particular, where fuel is needed to power backup generators, (Maron, 17).

II. Fears of Mideast Oil Pricing and Unrest

Fears of geopolitical unrest in the Middle East have caused a fluctuation of oil prices going back for several decades. Kinetic military actions and intelligence activities in the CENTCOM Area Of Responsibility (AOR) including Iraq, Kuwait, Qatar, Syria and Iran have been driven in part by national interests in crude oil reserves, (Lopez 52). In addition to traditional kinetic warfare "boots on the ground" actions, our exposure to cyber attack retaliation is real and impending.

This economic uncertainty can and should fuel a range of technological alternatives here at home. Indeed, home-grown renewable consumer vehicles have succeeded in the marketplace, including the Toyota Hybrid, Tesla Model S and the Tesla Roadster. Unfortunately, Big Oil has traditionally defended its own interests in profitable sales of crude oil, while creating a barrier to entry for startups who wish to innovate in renewable technologies, (Clarke 70). At present, the nation is experiencing a relaxation of crude oil prices, resulting in the lowering of gas prices at the pump. This surplus in OPEC supply is expected to last until 2017, (Maron).

III. Campaign Promises, Promises, Promises...

The Republican platform in dealing with cybersecurity vulnerabilities in our nation's infrastructure is complex, wide ranging, and unfortunately inferior to the need for action. John McCain of Arizona, Kay Bailey Hutchison of Texas and Chuck Grassley of Iowa have introduced the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act, which would "...promot[e] collaboration and information-sharing, updating our criminal laws to account for the growing cyber threat and enhancing research programs to protect our critical networks, " said John McCain in a statement, (Gross, 65). Unfortunately the central idea in the SECURE IT Act would call for a voluntary call to action on the organization's part, while not actually reinforcing the central mandate needed for effective security.

Meanwhile, on the other side of the political aisle, two Democrats, an independent and a Republican have introduced The Cybersecurity Act of 2012 as outlined and mandated in President Obama's State of the Union Address of 2012, [SOTU]. The Cybersecurity Act would allow the Secretary of Homeland Security to officially designate certain private networks as critical infrastructure, and require security plans to be submitted for the agency's review. It's worth noting that subsequent events including the hacking of retail stores in 2013-2014 prompted a review of the bill's intent, and the most recent successor to cybersecurity policy, the Cybersecurity Information Sharing Act (CISA) of 2015,

which is "...[to] improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes". This bill would allow the secretary of the U.S. Department of Homeland Security to designate some private networks as critical infrastructure and require them to submit security plans to the agency. But the SECURE IT Act (sponsored by McCain R-AZ, Hutchinson R-TX, and Grassley R-IA) has no such regulations, instead focusing on encouraging private companies and the federal government to share more information about cyberthreats, sponsors said.

IV. Paris 2015 Climate Change Talks

The 2015 United Nations Climate Change Conference, COP 21/CMP 11 was held in Le Bourget, France from November 30 to December 11, 2015, only a couple weeks after a major terrorist attack in Paris, France on 11/13 from ISIS, a major cyberterrorist group. Record world leader attendance (165 Signatories and 196 Ratifiers) demonstrated the wide significance of participation, versus prior conferences including the Bali Action Plan (2007), the Copenhagen Accord (2009), the Cancún agreements (2010), and the Durban Platform for Enhanced Action (2012), (Chuck, 13).

Interestingly enough, also in attendance were Russia's Vladimir Putin and Chinese President Xi Jinping, (strange bedfellows with the United States when threatened with climate change) with specific regards to their past activities in the Ukraine and South China Sea, respectively.

V. Wars Over Limited Resources

A looming battle remains over the increasing availability of oil reserves in the Arctic Ocean. A potential conflict between Alaskan, Greenlandian, Russian and Canadian territorial claims place the United States under a threat of conflict over petroleum resources in the Arctic. Potential oil reserves are now accessible with the withdrawal of arctic and antarctic ice shelves due to global climate change as discussed recently in Paris. Local concerns regarding nuclear sites, use, and waste material disposal concerns include Coldwater Creek and West Lake Landfill in North County. While these local concerns do not pose an immediate threat of a looming cyber attack, it does heighten a localized awareness of responsible uses of nuclear power, as well as the consequences of its utility. The point? To eliminate conflict, war and potential 21st century cybersecurity infrastructure power plant and grid line supply attacks by using renewable energy sources and processes which would yield minimal waste.

VI. Busting Myths In Green Infrastructure Security

Part of the challenge in pushing through a green cybersecurity initiative is educating the public of the benefits of having a more secure environment from which to generate a prosperous economy. Three items in particular struck this paper's author as particularly worthy of refutation: that of costs, safety, and reliability.

For those who believe in a prohibitive cost barrier to entry into the market, a strong counterargument would include the cost of inaction. Pretending that things are going to be OK if we do nothing, are oblivious to the facts presented. Economic incentives and tax savings are available, and the markets are also gaining more traction as companies and organizations realize the potential for profits while increasing the quality and reliability of their product.

Safety and security, another hot topic, is the focus of this paper. Political dependence on foreign crude exports binds us to risky investments and literally fuels a need for domestic production. Because of the plentiful nature of renewable resources, it is in our national interest to continue to invest in the harvesting of solar, hydroelectric, geothermal and wind energy as soon as possible.

To areas of the globe that may have plentiful resources at their disposal, it is essential to share with neighboring geographical areas the power that is produced in a local grid so that outages are minimized. This will enhance 24/7 reliability of the national power grid, where the key is to have a mix of sources spread over a wide area: solar and wind power, biogas, biomass and geothermal sources. In the future, ocean energy can contribute too.

VII. Conclusions and Final Thoughts

Investing in clean and renewable energy sources increases our safety and cybersecurity defense posture by making affordable and available the reliability and security needed in the 21st century and beyond. By increasing the utility and convenience of renewable technologies, we enhance and strengthen our national economy and infrastructure by reducing our external influences and political dependencies on commodities made vulnerable by risk of conflict or by eventual depletion of finite resources. Therefore it is in our national interest to learn more about renewables in order to take advantage of them, and for our society to prosper from them, moving forward.

REFERENCES:

Chuck, H. (2015, December 1). Chuck Hagel: Climate Change Is a National Security Problem. *Time Magazine*.

Clarke, R., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it.* New York: Ecco.

Gross, G. (n.d.). "Republican Senators Introduce Their Own Cybersecurity Bill" *PC World*.

Lopez, J., & Setola, R. (2012). *Critical infrastructure protection information infrastructure models, analysis, and defense*. Berlin: Springer.

Maron, D. (2010, October 18). Can Renewable Energy Make U.S. Military Bases More Secure? *Scientific American*. Retrieved December 2, 2015, from http://www.scientificamerican.com/article/can-renewable-energy-make-us-military

Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 3681, 112th Cong. (2012).

Walsh, J. (2011, June 22). Under the Arctic Ocean, a Great Sea of Oil Awaits; Greens Fear the Push for Black Gold. *The Washington Times*. Retrieved November 16, 2015, from http://www.highbeam.com/doc/1G1-259488978.html

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon.* New York, New York: Crown Publishing Group.