The Predator's View: The Imperative for Critical Infrastructure Resilience

by JEFF GAYNOR, Colonel, U.S. Army (ret.)
Director, Board of Directors, InfraGard National Members Alliance

CIRCA 1832, PRUSSIAN GENERAL AND MILITARY Theorist Carl Von Clausewitz noted[1] : "War is not merely an act of policy but a true political instrument, a continuation of political intercourse carried on with other means." Long before Clausewitz and to this day, adversaries have sought and seek to identify, corrupt, disrupt, degrade or destroy capacities that enable their foes to inflict their will and objectives. America's decades-long efforts to protect, and with the February 2013 publication of Presidential Policy Directive 21 (PPD-21), ensure "Critical Infrastructure Security and Resilience," demands awareness, understanding and appreciation of the *"predator's view*[2] ." Adversaries see America, Americans, and/or anything contributing to the nation's safety, security, quality of life and future, as ***legitimate targets***. Given their inherent capacities to both empower and inflict consequences, this is especially true of America's interdependent critical infrastructures — cyber and physical.

[1] Clausewitz: "On War"
[2] Homeland Security Advisory Council, Critical Infrastructure Task Force Report, January 2006

The absence of understanding and appreciation of the *predator's view* has been evident throughout history. In 410 AD, the Goths laid siege to Rome and captured it after identifying aqueducts as a *single point of failure* whose degradation would halt the flow of water into the city and thereby eliminate any resistance within it. In 1943, a Norwegian hydrogen plant producing "heavy water" was attacked and destroyed by Allied Saboteurs[3] and a subsequent raid by 140 U.S. bombers. Not unlike Rome's aqueducts, the plant was a *single point of failure* whose destruction (and the subsequent sinking of the Norsk, a ferry transporting the remaining inventory of heavy water) effectively terminated Nazi efforts to build an atomic bomb. Conversely, Japanese failure to neutralize critical infrastructures is evident in their December 7, 1941 attack upon Pearl Harbor. While Japan scored a stunning tactical victory along Battleship Row, its failure to attack maintenance and fuel storage facilities adjacent to it (then a *single point of failure* for the Pacific Fleet) was a strategic blunder that greatly accelerated the demise of the Japanese Empire.

Fast forward to the Information Age. In the aftermath of Operation Desert Storm and America's and her Allies' stunning victory over Iraq's Army (then the world's fourth largest), the Chinese People's Liberation Army initiated a study that is captured in its 1998 publication, "Unrestricted Warfare." The study concluded that information was the key to the American and Allied victory and offered means to neutralize what could be termed "America's Nervous System." As a result, the Chinese (and any predator engaged in cyber probes and attacks) understand that it is no longer necessary to physically destroy a technology-reliant nation to inflict its will upon it. They have discovered a more antiseptic and efficient approach: attack interdependent and cyber-reliant critical infrastructures and produce consequences of potentially unprecedented scope, intensity and duration and, in the process of doing so, degrade social cohesion — the heart of a nation's ability to defend itself. From the *predator's view*, validating that approach is its recognition of a valuable contradiction: America's rapidly increasing reliance on the Internet and supporting telecommunications capacities is significantly outpacing its ability to assure their availability and security. The predator's conclusion: America is the most Internet-reliant nation on Earth and for whatever reason is creating the instrument of its demise, its own Achilles Heel — a single point of national failure.

Consistent with this reality, FBI Director James Comey has repeatedly and very correctly warned: "Cyber is not a thing — it's a vector[4]. " Despite popular perception that the Internet has evolved into an "Internet of Things," the truth is it has become "The Internet of American Life." As evident from near daily press accounts, all manner of global cyber predators routinely and successfully probe, map and attack the information infrastructure that is "America's Nervous System." The nation therefore now finds itself at the crossroads of Internet reliance and availability.

America is the most Internet-reliant nation on Earth and for whatever reason is creating the instrument of its demise, its own Achilles Heel – a single point of national failure.

Any continuity professional will warn that it is both illogical and irresponsible to rely on something over which you have limited or no control. While the term "lessons learned" is frequently used in America as a means of cognitively balancing catastrophic events, predators know the real metric of a *lesson learned* is a change in behavior and conditions at points of actual or potential impact. From the *predator's view*, America has consistently produced only changes in rhetoric. Predators appreciate America's use of terms like "Cyber Pearl Harbor," "New Normal," and the "Internet of Things." They recognize that such characterizations understate reality and are useful in pacifying the masses and slowing efforts to eliminate vectors otherwise increasingly capable of inflicting human, physical, economic and social consequences of unprecedented scope, intensity and duration.

There are numerous examples of predator success in *walking their talk*. Among them are:

[3] "The Heroes of Telemark"
[4] International Conference on Cybersecurity, Fordham University, January 7, 2015

1. China's aggressive behaviors in the Pacific and its version of the F-35, America's most advanced stealth strike fighter;
2. Russia's employment of Cyber Warfare in Georgia and the Ukraine;
3. Russian and/or Chinese attacks against State Department and White House networks; and
4. Secretary of State John Kerry's remarks: "It's very likely Russia and China are reading my e-mails.[5]"

Through predators' eyes, great reliance enables great consequence. The *predator's view* is long and patient. They perceive America as living in the moment rather than in the reality and continuity of time and history. While recognizing English is a very flexible language, predators also see in America's rhetoric a homogenization of otherwise incompatible terms. Specifically, its equation of *iteration with innovation, process with progress, activity with accomplishment, and rhetoric with results*. From the nation's habit of providing timely and accurate reporting of the effects of attacks on America's Nervous System (its information infrastructure), predators recognize our apparent tolerance for infrastructure degradation and failure, tendency to *rationalize* events and equate the absence of immediate consequence(s) with success in preventing them.

Through predators' eyes, great reliance enables great consequence. The *predator's view* is long and patient. They perceive America as living in the moment rather than in the reality and continuity of time and history.

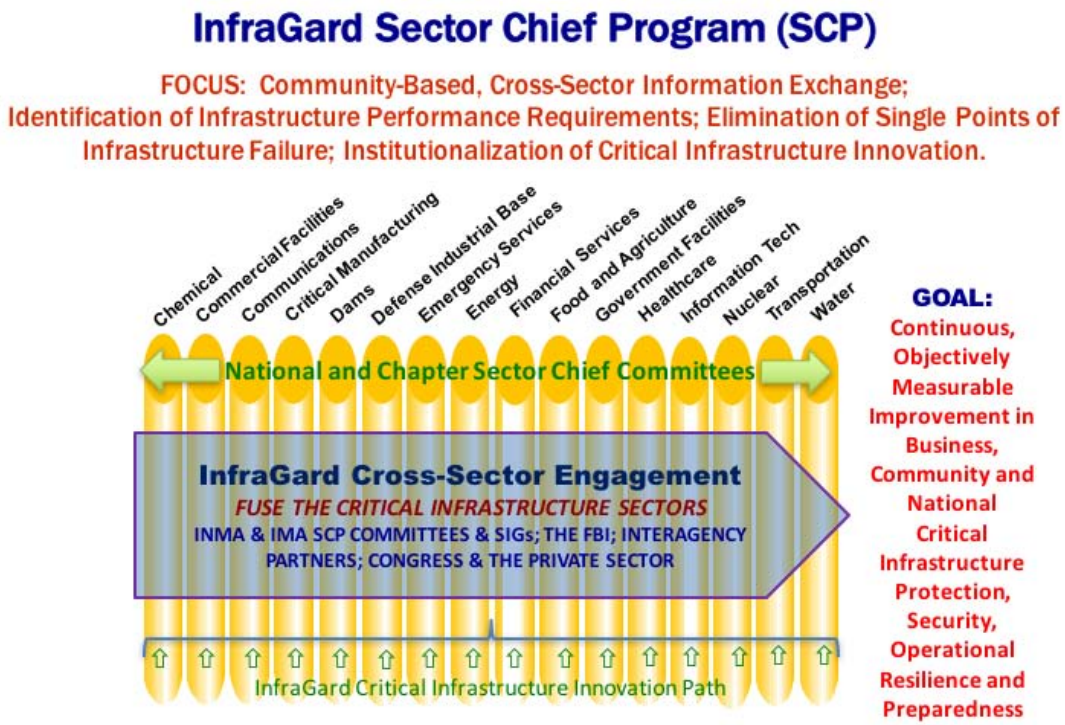
The *predator's view* and the trajectory of infrastructure preparedness have not gone unrecognized. Over a decade ago, in the midst of the continuing consequences of a long-predicted failure of a critical infrastructure and single point of community failure in New Orleans, the Homeland Security Advisory Council's (HSAC) review of critical infrastructure protection programs resulted in its formal recommendation that the Homeland Security Secretary make Critical Infrastructure Resilience (CIR) the national goal[6]. Three years ago, that goal was captured in Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience." While these documents very clearly set the requirement, progress in physically achieving CIR remains obscure at best. Operationally proven CIR mindsets, metrics, methodologies and technologies have been and remain immediately available for implementation. The decision to execute will herald and be the foundation of an advanced infrastructure and national preparedness culture that is performance-based, comprehensive, nationally compatible, objectively measurable, achievable and sustainable. Given increasing predator exploitation of the "vector" the Internet has become, achieving and sustaining CIR is now the most fundamental and urgent of homeland and national security goals.

Among others, President Ronald Reagan captured the dangers of not eradicating dangers: "Status quo you know is Latin for the mess we are in[7]." Given the above and far more, the question remains: How does America clean up ". . . the mess we are in?"

The good news is that despite the current and rapidly mounting dangers looming on its horizon, America has the experience (among others, the Year 2000 Transition), ingenuity and means to deal with existential threats to its cyber-reliant critical infrastructures. CIR is an advanced infrastructure preparedness condition that is symbiotic with existing critical infrastructure sector organization, protection and security programs. CIR, like anything built to last, is constructed and maintained from the ground up. In this case, from American communities, where all interdependent infrastructure operations naturally fuse and from where knowledgeable infrastructure performance requirements are set, single points of infrastructure failure are identified and eliminated, and (beyond information sharing) actionable, trust-building, question and answer-based *information exchange* originates.

With 50,000+ members deployed in 84 communities throughout the nation, InfraGard chapters work in concert with local FBI Field Offices and constitute America's greatest resource for achieving and sustaining CIR — and by extension — national resilience. InfraGard members represent infrastructure service providers, businesses, local and state government agencies, academic institutions, emergency responders, faith-based organizations and state, local and federal law enforcement

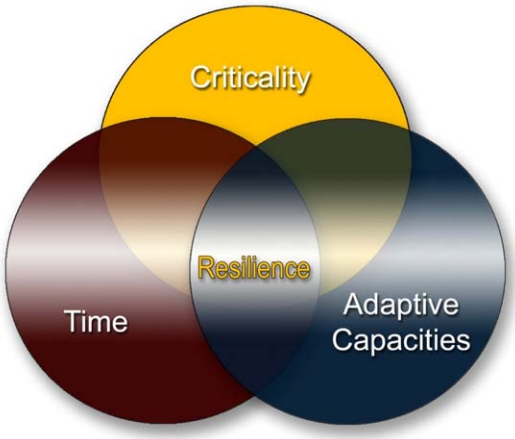
[5] CBS Evening News, August 11, 2015
[6] "Homeland Security Advisory Council Report of the Critical Infrastructure Task Force"
[7] www.brainyquote.com/quotes/quotes/r/ronaldreag183973.html



agencies - all of which support the continuity of infrastructure operations in all 16 interdependent infrastructure sectors.

InfraGard's Sector Chief Program and Special Interest Groups at the local and national levels form a network that provides proven experience and expertise in both sector and cross-sector issue identification and resolution, and in the institutionalization of continuous innovation and improvement in the protection, security and resilience of the nation's critical infrastructure(s).

Combined, the expertise and placement of InfraGard members throughout the nation advances the ability of the FBI and its federal partners to identify and address threats to America's critical infrastructure(s), and identify infrastructure performance shortfalls and *single points of failure* throughout the nation. InfraGard is also a key source of the timely, accurate and actionable information required to attain and sustain the security and operational resilience of America's critical infrastructures — to include the creation of a *Minimum Essential National Infrastructure* that, true to its name, will (short of Global Armageddon) provide sufficient infrastructure capacities to sustain American life. In a nutshell, InfraGard meets the spirit, intent and letter of what Governor Tom Ridge, the first Department Homeland Security (DHS) Secretary, had in mind when he set the Department's mission culture, created and led DHS's execution of the following



maxim: "When America's hometowns are secure, the homeland will be secure."

Turning to CIR execution, Einstein is quoted as saying: "If you can't explain it simply enough, you don't understand it well enough." Consistent with that truth, the objectively measurable and operationally proven CIR process is captured in the Venn diagram above.

CIR implementation requires entities ranging from individuals and businesses to communities, regions and the nation to:

1. Identify the cyber and physical infrastructure

capacities that are critical to their daily lives and operations;
2. Decide how long (time) any entity is willing to be without what is critical to it; and
3. Identify and/or create the *adaptive capacities* required to deliver critical infrastructure capacities within the time any entity is willing to be without them.

When implemented, CIR provides for the "predictable provision of essential infrastructure products and services and empowerment of essential functions©[8]." It is a proven, pragmatic, risk-based, performance-driven, nationally comprehensive and compatible, achievable and sustainable infrastructure operating and preparedness standard. Its achievement will leverage the power inherent in America's freedoms and its citizens' independence, innovative spirit and technological supremacy. The continuous application of resilience mindsets, improvement effected by always questioning the status quo, its metric (time), methodologies (illustration above), and innovations (e.g., cyber indications and warning), will:

1. Balance a national preparedness culture that is currently heavily focused on response and recovery; and,
2. as General Russel Honoré, Task Force Katrina Commander, noted: will get America to ". . . the left side [prevention and continuity of operations] of the event horizon."

While time is the metric of resilience, it is no longer on America's side. The critical infrastructure *reliance* culture must be replaced with a critical infrastructure *resilience* culture that continuously:

1. Identifies and eliminates all single points of infrastructure failure;
2. Distorts "the predator's view";
3. Reduces infrastructure target values and the immediate and cascading consequences of attacks upon, or failures of, those targets regardless of cause;
4. Informs coherent investment in critical infrastructure (to include creation of a *Minimum Essential National Infrastructure)*;
5. Creates an *American Renaissance* - a culture and resulting actions that enables continuous infrastructure innovation, investment and robust job creation to modernize and make resilient America's infrastructure foundations and all they empower; and
6. Builds national unity by enabling all Americans to work simultaneously in their best interests and ultimately in the best interests of all.

BOTTOM LINES: Sober recognition, understanding and appreciation of the *predator's view* are the first steps in countering their objectives. What Americans take for granted as things common to our everyday lives, predators of all stripes from the "lone wolf" to nation-states and their allies, view as legitimate targets. The question remains whether CIR will be executed proactively and with precision or reactively and chaotically in the wake of yet another otherwise preventable tragedy.

America has the responsibility and ability to correct its increasingly infrastructure-enabled and consequence amplifying preparedness trajectory. In the process of doing so, America will disrupt the designs of global predators, reclaim control of its enablers, and build the foundation for a safer, stronger and more secure nation for present and future generations.

About the Author

Jeff Gaynor is a uniquely experienced retired U.S. Army Colonel, Intelligence and Counterintelligence Officer, and Silver Star recipient whose national security career spans over a half-century. With over 30 years of enlisted and commissioned service, Jeff's uniformed assignments ranged from Army Communications Monitor to Advisor to Vietnamese Territorial Forces, and to the White House as the Communications Security Officer and Alternate Military Aide to Presidents Ronald Reagan and George H.W. Bush. Upon retiring from active duty, Jeff continued his service to the nation as a Department of Defense Department (DoD) Civilian as the Principal Action Officer for the creation of the Defense-wide Information Assurance Program.

Appointed as a Defense Intelligence Senior Executive, Jeff directed the Department's Year 2000 (Y2K) Operations and became its first Principal Director for Security and Information Operations. In the wake of the attacks of September 11, Jeff served as a Special Assistant for Homeland Security and Defense Intelligence Liaison to the White House. He later created and directed Homeland Security Senior Advisory Committees for the President's

[8]

Homeland Security Advisory Council and Homeland Security Advisory Council (HSAC). In March 2005, Jeff created and directed the HSAC's Critical Infrastructure Task Force (CITF). In the wake of the devastation wrought by the failure of the New Orleans Levee System, the HSAC's January 2006 report called for and provided an advanced, performance-based infrastructure preparedness standard (Critical Infrastructure Resilience). The report remains recognized as: "The Foundational U.S. Government document on Critical Infrastructure Resilience."