Journeyman Jihadism

Are Americans More Secure Now?

Terrorism's Tempting Targets
At 1300 EST today, four members of a splinter terrorist organization activated a US-based cell to carry out an attack on the nation's capitol using an RDD or a "dirty bomb". They chose cesium-137 because of its availability, high radioactivity, high dispersability, and the difficult nature of clean up and remediation. Their goal was a highly visible attack creating death to the maximum extent possible, as well as inciting fear, social, and economic disruption. Using a rented panel truck, the terrorists detonated a 3,000 pound bomb containing 2300 curies of cesium in the downtown government district near the Ronald Reagan Center. The explosion collapsed the front of the building and caused severe damage to three others. Windows were blown out of five other buildings. Amid the destruction, cesium contamination now covers the scene and the contaminated detonation aerosol was lifted over 100 feet into the air. Foot and vehicular traffic after detonation have re-suspended and transferred contamination for more than five hours – now contributing to contamination spread beyond the 36 square block primary zone. People who were initially in the primary zone escaped in the first few minutes using the metro and are now taking contamination home with them in their hair and clothing. Small fires from ruptured gas utility lines are burning in the vicinity of the blast. Unstable building facades, rubble, and broken glass now create physical hazards for rescue workers. Small amounts of lead and asbestos are present in the air and on surfaces. Human remains are presenting a significant radioactive biohazard.

Botnets have also unleashed a massive intrusion on the capitol regions virtual infrastructure crashing the servers of several federal agencies and will effectively close down the electrical power grid in a matter of hours.
Media vehicles have converged onto the scene and are attempting to initiate standoff broadcast

National Guard CBRN and FEMA groups are attempting to contain the situation but are struggling with the coordination of federal and local first responder teams and assets. Cellular telephone service has completely collapsed and radio frequencies appear to be jammed due to electromagnetic pulse interference effects believed to be connected to the detonation. In what is undoubtedly a coordinated effort, coverage of the attack from a still undefined and growing perimeter around the contamination zone . . .

Note: In the confusion of the first hours, the original news media report was only of a chemical attack. Although they got it wrong in the beginning, the attack required CBRN teams as first responders.

Can That Really Happen?

The current race to elect of our next supreme commander includes the basic question for all americans, do you feel safe? The scope of this contemplation might also include an assessment of your hollistic views of what is loosely called "the war on terror" when further analysis reveals the irregular war(s) are engaged with radical islamic groups who are often even each others adeversaries.

While this is only an attack scenario, it is intended to illustrate the degree to which the U.S and other developed nation states still remain vulnerable to "man-made disasters" (in the vernacular of the USG) years after 9/11. Of greater concern is the present threat environment within the gaps of the maritime domain and corresponding mission areas and conops for infiltration methods, targets and plausible crisis scenarios that could become reality through the efforts of non-state actors and determined extremists who prefer acts of terror over direct confrontation with the U.S. military.

Two If By Sea?
It was only November of 2008 when a militant organization based in Pakistan and suspected of ties with Indian militants arrived in Mumbai harbor using common small watercraft laden with assault weapons, grenades, and bombs. Without warning they struck at multiple landmark-like targets (including hotels, public buildings and transportation choke points) killing 179 and wounding more than 300. Indian authorities not only failed to detect the threat but were criticized for their apparent inability to mobilize against the attackers with enough force and speed to prevent the scale of damage and loss of life achieved by the infiltration. A post-attack assessment revealed that the assailants were able to easily enter the crowded port undetected through the use of small boats that blended in with local fishing activities. Hotels and other key infrastructure were totally unprotected with neither security features nor forces. The lack of integrated communications with central command and control interoperability amongst responding agencies also delayed response time, created confusion, and prevented the adequate coordination of resources.

Security analysts in the US have since deconstructed the attack and others like it and determined that the group or other militants using similar tactics could succeed with strikes that target public spaces adjacent to major waterways in this country as well.

90 percent of our imports and exports move by sea . . . ports are our economic lifeline . . .

Success Breeds Confidence
The 9/11 attacks illustrated with terrifying clarity how determined terrorists will use any type of conveyance to prosecute their strike mission in the name of Jihad.

With an astounding success record, low cost, ease of operation and ability to hide amid the clutter of commercial and recreational vessel traffic – small boats are expected to rapidly emerge as the vehicle of choice for militant infiltration and attack schemas.

For example, today most watercraft operate with surprising impunity near high-priority commercial vessels such as liquefied natural gas (LNG), oil tankers and containerized cargo vessels – and could be employed in a suicide attack as was the case in Yemen in 2000. The USS Cole, a US military DDG

class vessel was rammed by an explosive carrying small dinghy killing 17 sailors – al Qaida operatives took responsibility for the brazen attack.

The Breeze is Terrific

The geography of the United States includes slightly more than 95,000 miles of waterline – either coastal or river banks. Over the course of three centuries, many of the countries major cities and economic centers have been built adjacent to major water ways for a very basic reason: 90 percent of our imports and exports move by sea – ports are our economic lifeline. Ports also support some of our most critical and hazardous infrastructure facilities. The fact is, port facilities are among the most attractive targets for creating large-scale economic and social disruption.

Vehicle	Mission	Outcome
Small craft	Infiltration	Discharge of operatives and weapons
Pleasure boat or small craft	Smuggling	Delivery of WMD, CBRN
Pleasure boat	Suicide Attack	Destruction of port facilities & commerce
Small craft	Suicide Attack Military Target	Create media attention
Unmanned underwater vehicle	Suicide Attack	Destruction of port facilities & commerce
Semi-submersible vehicle	Smuggling	Delivery of WMD, CBRN
Small craft	Piracy, hostage seizure	Ransom demands
River craft	Smuggling	Delivery of materials and or information

Boston's harbor is not unlike many similar ports located near major population centers such as Seattle, Long Beach, New Orleans, Miami, Newark, and Chicago. These examples all share several common traits including the routine transiting of very large vessels containing flammable cargos (Long Beach and Newark), large containerized cargo import and export operations (Miami and Newark) and significant public space and population buildup adjacent to the waterline (Seattle and Chicago). In fact the sheer size and density of the Seattle waterfront buildup creates an area so vast it is likely impossible for the Seattle Port Police to monitor and defend. In addition, potential adversaries have a broad range of approach routes due to the myriad of coastal waterways and inland-sea passages.

A Question of Next?

Americans continue to take reckless risks while eschewing potential consequences. Oil refineries and chemical processing plants still operate in dangerous proximity to dense population centers. Our electrical grid continues to deteriorate while demand for power to supply computers and ventilation systems grows. And our investments in monitoring technology and providing surge capacity for first responders is frighteningly small compared to the sum spent on military programs and operations.

Protecting ports and coastal population centers from hostile boats remains a considerable challenge for U.S. agencies. An estimated 13 million recreational water vehicles operate within three million square miles of littoral and river waters providing ideal cover for adversaries to hide amid the maritime congestion. As the Coast Guard, DHS and local agencies plan for contingencies, it appears that the question of water vehicle infiltration countermeasures will see further advancements as long as this lethal threat can compromise national security.

The Rise Of The Super Empowered Non-State Actors

During a recent presentation at a "Mad Scientists" gathering hosted by the US Army, attention was drawn to the looming menace posed by Super Empowered Individuals (SEIs) during the Visualizing Multi-Domain Battle 2030-2050 Conference at Georgetown University.

Within this discourse, the Army underscored algorithmic warfare and the specter of bio-chemical assaults as paramount threats confronting our national security amidst a myriad of potential attack vectors accessible to both state and non-state actors. By the year 2040, the pervasive influence of machine learning is anticipated to revolutionize global economies, fundamentally reshaping labor dynamics—a pivotal factor with profound implications for global stability.

Characteristics inherent to super empowered individuals encompass heightened connectivity, enabling them to transcend geographical confines, alongside access to potent yet affordable commercial technologies. This accessibility renders them elusive entities, challenging conventional methods of traceability and attribution. Unbound by nation-state norms, ethical frameworks, or international legal statutes, these individuals harbor diverse motivations ranging from political and ideological to economic and pecuniary.

The actions of super empowered individuals often defy predictability, deviating from the rational behavior typically associated with traditional actors. Engaging in multi-domain battles with such entities raises novel ethical and legal quandaries. Questions arise regarding the delineation of acts of war in a landscape where human organization transcends national boundaries. Furthermore, identifying algorithms as adversaries or allies poses an intricate conundrum. Ambiguity shrouds whether an attack by a super empowered individual against individuals or entities warrants law enforcement intervention or Pentagon involvement, exacerbating the complexity of the issue. Similarly, the release of tailored viruses prompts speculation over whether such actions constitute acts of war, hate crimes, or fall under different classifications altogether.

> “What are the boundaries associated with conflict between nation states and super empowered individuals?”

Experts concur that SEI-driven threats are poised to become increasingly prevalent with the proliferation of advanced and disruptive technologies. The arsenal of these individuals encompasses a spectrum of tools, from powerful 5G smartphones doubling as multi-spectral sensors to commercial UAVs repurposed as precision-guided kamikaze munitions. Moreover, the weaponization of high-powered computers with

debilitating malware and ransomware poses a grave threat. Information warfare and psychological manipulation through social media platforms have not only influenced policy but also disrupted societal norms, escalating global security concerns. Simultaneously, Distributed Denial of Service (DDoS) attacks have debilitated both businesses and governmental institutions at various echelons. The advent of advanced cyber capabilities, coupled with the widespread availability of lethal technologies and associated tactics, affords super empowered individuals the capacity to disrupt, degrade, and deny multiple domains—be they social, commercial, or military—at will. Consequently, a solitary individual or group equipped with proficient coding and hacking skills could inflict commensurate damage to that of a conventional armed force. The looming prospect of future SEIs acquiring technologies and methodologies currently the purview of intelligence agencies further compounds national and global security apprehensions, with uncertainties persisting regarding states' capacity to counter or deter such malevolent applications of technology.

The ascendancy of super empowered individuals, capable of delivering effects previously only within the realm of state actors, engenders critical inquiries concerning the definition of acts of war:

What delineates conflict between states and super empowered individuals?

How does the military address surveilling, targeting, and engaging super empowered individuals outside of current counterterrorism policy, regulations, and doctrine?

The potential of super empowered individuals to wield substantial influence in shaping the future is undeniable. Consequently, the Pentagon must delineate a clear strategy to address and neutralize this burgeoning threat.

It is plausible that certain super empowered individuals have already coalesced into organized groups, pooling their respective capabilities and interests to pursue power, control, and financial gain while advancing collective ambitions.

Images

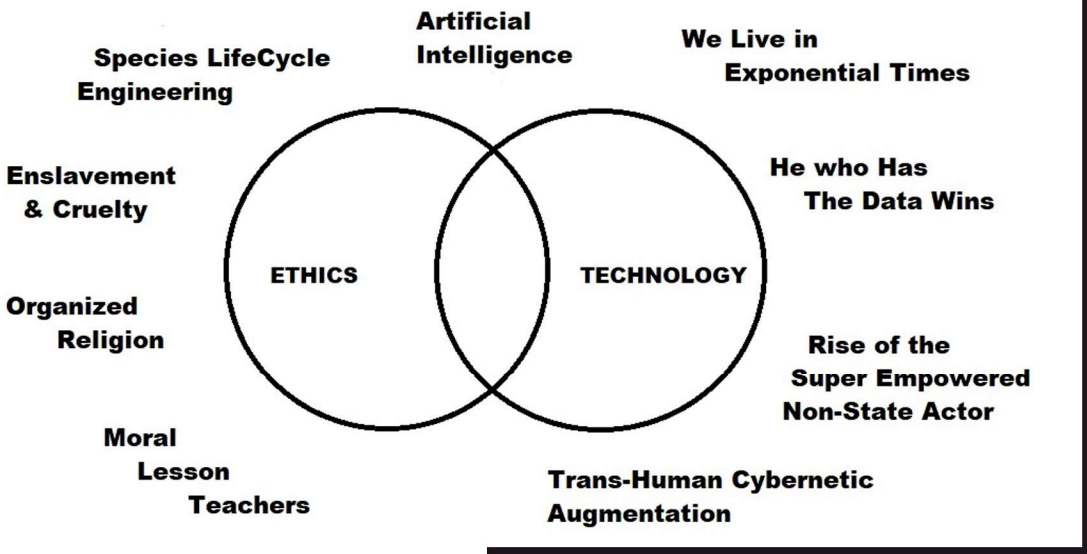
George Soros is a Hungarian-American billionaire hedge fund manager and philanthropist and is known as “The Man Who Broke the Bank of England” as a result of his short sale of US$10 billion worth of pounds sterling, which made him a profit of $1 billion, during the 1992 Black Wednesday UK currency crisis.

Viktor Anatolyevich Bout is a Tajik-born Russian arms dealer who used his multiple companies to smuggle arms from Eastern Europe to Africa and the Middle East.

Conspiracy Theory 2050

ABOUT

Conspiracy Theory 2050 is created and published by PWK International Advisors, a Boston based advanced technology practice that helps organizations of all sizes to identify build and sustain the capabilities they need to continuously improve performance and deliver impact with frameworks powered by advanced technology.



Design by David Tashji

PWK INTERNATIONAL ADVISERS

www.pwkinternational.com