MAD SCIENTIST LABORATORY
… Exploring the Operational Environment

JANUARY 2, 2018 BY USER

16. Emergent Threat Posed by Super-Empowered Individuals

"… in calling Moriarty a criminal you are uttering libel in the eyes of the law, and there lies the glory and the wonder of it! The greatest schemer of all time, the organizer of every deviltry, the controlling brain of the underworld — a brain which might have made or marred the destiny of nations. That's the man!" Sir Arthur Conan Doyle's Sherlock Holmes, describing his arch nemesis, Professor James Moriarty, in **The Valley of Fear**, published in 1914.

In Professor Moriarty, Conan Doyle created the prototypical Super-Empowered Individual (SEI). Today's SEIs — far from being fictional characters crafted to entertain readers from a gentler era — are real world, non-state actors that have been empowered by the on-going digital revolution, and are able to target and adversely affect the lives of millions around the globe. Mad Scientists addressed the threat posed by SEIs at the **Visualizing Multi Domain Battle 2030-2050** Conference, Georgetown University, 25-26 July 2017.

Per NIH, 1-2% of humans exhibit psychopathic behaviors

extracted from Dr. David Bray's presentation at Georgetown University (see link at bottom of this post)

Characteristics of SEIs include:

• Highly connected and able to reach far beyond their geographic location.

• Access to powerful, low-cost commercial technology.

• Often more difficult to trace or attribute responsibility to actions.

• Not beholden to nation-state policies, ethics, or international law.

HOT!!!

Click **here** to review the TRADOC G-2's draft information paper **The Operational Environment (2021-2030): Great Power Competition, Crisis, and Conflict**, then drop us an email at **madscitradoc@gmail.com** and give us your feedback!

Click **here** to read the Army Future Command's new **AFC Pamphlet 525-2, Future Operational Environment: Forging the Future in an Uncertain World 2035-2050** addressing the mid- to far term OE and watch the associated **video**!

Watch the TRADOC G-2's new **The 2 + 3 Threat** video addressing the near-term OE (i.e., 2020 to 2028)!

Watch the new **TRADOC 2028** video [via a non-DoD network]!

PRIMERS ON THE OPERATIONAL ENVIRONMENT

The Changing Character of Future Warfare video

TRADOC Pamphlet 525-92, The Operational Environment and the Changing Character of Warfare

Potential Game Changers handout

TP 525-92-1, The Changing Character of Warfare: The Urban Operational Environment

The Arctic Through 2035: An Overview of the Operational Environment and Competitor Strategies for U.S. Army Training, Doctrine, and Capabilities Development

The Information Environment: Competition & Conflict anthology

MORE OPERATIONAL ENVIRONMENT RESOURCES…

Foreign Military Studies Office OE Watch

Watch The Future of Unmanned Maritime

• Varying motivations (political, ideological, economic, and monetary).

• Often unpredictable, may not operate or execute like a traditional rational actor.

SEI-driven attacks will become increasingly common due to the proliferation of disruptive technologies — smart phones as multi-spectral sensors and jammers; commercial UAVs as precision-guided munitions; and high-powered computers with malware / infoware "weapons" — available to them.

This has been evidenced by the rise in global malware attacks, hacking of vehicles that operate with computers, and information operation campaigns through social media that have influenced policy, disrupted everyday life, and increased global security costs and concerns.

Wired recently reported on several Distributed Denial of Service (DDoS) attacks, launched by SEIs. This **article** reports that three college students have plead guilty to creating and launching **Mirai**, *"… an unprecedented botnet—powered by unsecured internet-of-things devices like security cameras and wireless routers—that unleashed sweeping attacks on key internet services around the globe,"* slowing or stopping the internet for most of the eastern United States. Their motive – *"trying to gain an advantage in the computer game Minecraft."*

According to FBI Special Agent Elliott Peterson, **"DDoS at a certain scale poses an existential threat to the internet…. Mirai was the first botnet I've seen that hit that existential level."**

Cyber capabilities such as this, coupled with the widespread proliferation of deadly technologies and associated tactics, techniques, and procedures, provide **SEIs with the capability to disrupt, degrade, and deny Army forces across multiple domains and the reach to interdict them at home station, as well as while deployed.**

These attacks, however, need not necessarily be broad DDoS operations; SEIs can leverage these disruptive technologies to craft and execute **personalized warfare** attacks against key leaders, Soldiers, and their families' via pressure points (e.g., social media, commerce, work, and financial transactions).

An individual armed with a high-powered computer and proficient coding, programming, and/or hacking capabilities could induce as much damage as an entire battalion of conventionally-armed belligerent forces.

"THE CONVERGENCE" — ARMY MAD SCIENTIST PODCASTS

Undersecretary of the Navy **James F. "Hondo" Geurts** and **Dr. Zachary S. Davis**, Senior Fellow, Center for Global Security Research, Lawrence Livermore National Laboratory, **discuss** *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Force* and how to think radically about the future, capitalize on talent, and unleash technological convergences to out-compete our adversaries, and when necessary, defeat them decisively in conflict.

COL John Antal (USA-Ret.), author and innovator in the interactive gaming and learning industry, **discusses** the implications of the Second Nagorno-Karabakh Conflict, the psychological effects of drone warfare, and the future of maneuver.

COL Scott Shaw, Commander, U.S. Army Asymmetric Warfare Group, **discusses** the future of ground warfare, including lessons learned from the Nagorno-Karabakh Conflict in 2020 and the realities of combat for tomorrow's Soldiers.

Dr. David Kilcullen, bestselling author and expert on unconventional warfare, **discusses** how the U.S. Army must prepare to engage "Dragons" and "Snakes" as they employ Liminal Warfare and blended cyber-kinetic operations to avoid our conventional warfare dominance.

Mr. Doowan Lee, Senior Director, Zignal Labs, **discusses** disinformation, changes over time in approaches to information warfare, and collaboration between Russia and the Chinese Communist Party on information operations.

Click here to listen to other episodes of "The Convergence"

MAD SCIENTIST PARTNER SITES

Modern War Institute Podcasts

Former Deputy Defense Secretary Robert Work Assesses the Future Battlefield

Dr. Moriba Jah on What Does the Future Hold for the US Military in Space?

Elsa Kania on China and its Pursuit of Enhanced Military Technology

Small Wars Journal Mad Scientist Page

U.S. Army War College War Room

Australian Army The Cove

Australian Defence College The Forge

SEARCH

These national and global security concerns are only worsened when future SEIs are able to obtain technologies and techniques that today are primarily limited to intelligence agencies. Meanwhile, states' ability to counter (or even deter) the malicious use of available technologies remains unclear.

SEI's ability to deliver effects previously limited to state actors raises the following questions regarding what constitutes an act of war:

• What are the boundaries associated with conflict between states and SEIs?

• How does the Army address surveilling, targeting, and engaging SEIs outside of current counterterrorism policy, regulations, and doctrine?

SEIs will impact the Future OE. The Army must address how it will address and counter this growing threat.

For further discussions on the ramifications of the digital age on geostability, see Dr. David Bray's presentation on **Blurred Lines and Super-Empowered Individuals: Is National Security Still Possible in 2040?** presented at Georgetown University.

ARMY MAD, ARMY MAD SCIENTIST, ARMY MAD SCIENTIST BLOG, ARMY MADSCI BLOG, FORECASTING THE FUTURE OF WARFARE, FUTURE OE, FUTURE WARFARE, MAD SCIENTIST, MAD SCIENTIST LABORATORY, MADSCIBLOG, SUPER-EMPOWERED INDIVIDUALS, TRADOC BLOG, TRADOC MAD SCIENTIST BLOG

---

2 Replies to "16. Emergent Threat Posed by Super-Empowered Individuals"

Dennis Woods CSM (R)
JANUARY 4, 2018 AT 10:43 PM

The Army must address how it will address and counter this growing threat presented by SEI's

One method would be to include them in the rules of engagement and general orders that relate to a given operation. This would allow leaders to react in real time with legal coverage for their actions

Reply

Machoman eller Eron Plus Verkan
JANUARY 11, 2018 AT 7:06 AM

Wonderful website. A lot of helpful information here. I'm sending it to several buddies and also sharing in delicious.
And certainly, thank you in your effort!

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

Could not connect to the reCAPTCHA service. Please check your internet connection and reload to get a reCAPTCHA challenge.