EXHIBITS

LIST OF EXHIBITS

I. **Journal Gazette newspaper article, 6/20/2017**
"False claims lead to real problems
Conspiracy theorist shuts down port"

II. **Transcript and certificates of FEMA sanctioned courses to demonstrate knowledge of the plaintiff in Critical Infrastructure Protection (CIP).**
FEMA transcript dated 6/22/2018 with three course certificates not appearing on FEMA transcript.

III. **A study of the Port of Charleston evacuation and closure: How Live Action Role Play (LARP) Simulations create Cognitive Threat Vectors", June, 2017, viewed 2,511 times. (https://www.slideshare.net/dgsweigert/port-of-charleston-evacuation-case-study-the-cognitive-threat-of-conspiracy-theorists)**

IV. **Report: Port of Charleston Dirty Bomb Hoax and Social Media Liability**

EXHIBIT ONE

The Journal Gazette
(/)

JGFRANK GRAY (/NEWS/LOCAL/FRANK-GRAY)

Tuesday, June 20, 2017 1:00 am

False claims lead to real problems

Conspiracy theory shuts down port

FRANK GRAY | The Journal Gazette

A couple of years ago, when the water in Fort Wayne started to taste funky as spring arrived and leaves and limbs were washed into the river, some people complained.

The water department assured everyone that the water was safe, it was tested several times a day, and it was using extra chlorine and charcoal filtering to minimize the earthy taste.

But not everyone was satisfied. Some went onto an internet site and, implying the water here wasn't safe, demanded an investigation.

That's what you can do with the internet, synthesize crises and send some people into a panic.

Last week, someone from Fort Wayne did the same thing again.

A man going by George Webb went onto a website he runs and claimed that a source had told him there was a dirty bomb planted in a major American city, possibly Memphis. He said the source had gotten his information from other "sources."

Before long the story changed to say there was a dirty bomb on a ship called the Memphis Maersk, a container ship headed for Charleston, South Carolina. That information ended up on another conspiracy channel on YouTube.

In the end, Webb, whose actual name is George Sweigert and who graduated from North Side High School in 1978, had managed to get the terminal evacuated where the container ship was located.

The Coast Guard inspected the ship and found nothing. It was another synthetic crisis. But it shows you what the internet can be used for.

That upsets a man named David Sweigert, who happens to be "George Webb's" brother and who graduated from North Side in 1977.

It's the result of what Sweigert, who is involved in infrastructure protection and computer security, says can happen when the internet is what he calls "weaponized."

Crowdsourcing sites that operate like games get fans to go online and solve mysteries and conspiracy theories, David Sweigert said in a paper he prepared after the event.

Participants are told of a threat, creating a call to action, and soon fans start calling authorities about the imminent threat, he said.

In the case of Charleston, the seaport had to be shut down.

You can call it a game, but when so-called journalists conducting what they call independent investigations get their listeners worked up, it can lead to player hysteria, angst and fear. David Sweigert compared the possible public reaction to the War of the Worlds Halloween broadcast in the 1930s, when some listeners were convinced the planet was being invaded by Mars.

The only difference now is that the broadcasts take place on the internet, and baseless attacks and public relations campaigns against public officials and infrastructure operators can develop.

The whole incident is troubling to him because it was all orchestrated, in part, by his brother.

What's at stake? False internet claims can incite violence, he said, against banks, utilities, dams, hospitals, name it.

Frank Gray reflects on his and others' experiences in columns published Sunday, Tuesday and Thursday. He can be reached by phone at 461-8376, fax at 461-8893, or email at fgray@jg.net. You can also follow him on Twitter @FrankGrayJG.

EXHIBIT TWO

FEMA

Emergency Management Institute – Independent Study Program
16825 South Seton Avenue, Emmitsburg, MD 21727 (301) 447-1200

STUDENT TRANSCRIPT

Last Name	First Name	MI	Student ID
SWEIGERT	DAVID	G	***-**-[redacted]

Issued: June 22, 2018

Course Code and Title		Completed	IACET CEUs*
IS-00001	Emergency Program Manager An Orientation to the Position	06/16/2011	1.0
IS-00001.a	Emergency Manager: An Orientation to the Position	06/11/2013	0.6
IS-00005.a	An Introduction to Hazardous Materials	01/24/2012	1.0
IS-00007	A Citizen's Guide to Disaster Assistance	06/08/2011	1.0
IS-00008.a	Building for the Earthquakes of Tomorrow	06/09/2011	1.0
IS-00015.b	Special Events Contingency Planning for Public Safety Agencies	03/02/2011	0.4
IS-00021.11	Civil Rights and FEMA Disaster Assistance	02/13/2011	0.1
IS-00022	Are You Ready? An In-depth Guide to Citizen Preparedness.	06/08/2011	1.0
IS-00027	Orientation to FEMA Logistics	02/14/2011	0.4
IS-00029	Public Information Officer Awareness	06/12/2018	0.2
IS-00033.11	FEMA Initial Ethics Orientation 2011	03/04/2011	0.1
IS-00035.11	FEMA Safety Orientation 2011	03/03/2011	0.2
IS-00038	Fraud Awareness & Prevention	10/15/2012	0.1
IS-00075	Military Resources in Emergency Management	03/02/2011	0.2
IS-00100.a	Introduction to the Incident Command System, ICS-100	06/07/2010	0.3
IS-00100.HCb	Introduction to the Incident Command System (ICS 100) for Healthcare/Hospitals	05/12/2011	0.3
IS-00100.LEa	Introduction to the Incident Command System, ICS-100 for Law Enforcement	06/07/2010	0.3
IS-00100.PWa	Introduction to the Incident Command System ICS-100 for Public Works	10/17/2008	0.3
IS-00101.b	Deployment Basics	02/03/2012	0.1
IS-00102.a	Deployment Basics for FEMA Response Partners	02/15/2011	0.1
IS-00102.b	Deployment Basics for FEMA Response Partners	02/03/2012	0.1
IS-00106.11	Workplace Violence Awareness Training 2011	02/14/2011	0.1
IS-00120.a	An Introduction to Exercises	05/26/2010	0.5
IS-00130	Exercise Evaluation and Improvement Planning	05/27/2010	0.5
IS-00139	Exercise Design	06/04/2010	1.5
IS-00144	Telecommunicators Emergency Response Taskforce (TERT) Basic Course	07/17/2012	0.3
IS-00200.a	ICS for Single Resources and Initial Action Incidents, ICS-200	06/03/2009	0.3
IS-00200.HCa	Applying ICS to Healthcare Organizations ICS-200 for Health Care/Hospitals	01/15/2012	0.3
IS-00201	Forms Used for the Development of the Incident Action Plan	02/03/2012	0.2
IS-00230.a	Fundamentals of Emergency Management	12/08/2009	1.0

Course Code and Title		Completed	IACET CEUs*
IS-00235	Emergency Planning	05/28/2010	1.0
IS-00235.b	Emergency Planning	01/05/2012	1.0
IS-00240.a	Leadership and Influence	02/13/2011	0.9
IS-00241.a	Decision Making and Problem Solving	06/06/2011	0.8
IS-00242.a	Effective Communication	02/13/2011	0.8
IS-00244.a	Developing and Managing Volunteers	02/13/2011	1.0
IS-00247	Integrated Public Alert and Warning System (IPAWS)	12/14/2011	0.2
IS-00248	Integrated Public Alert and Warning System (IPAWS) for the American Public	03/07/2018	0.0
IS-00250.a	Emergency Support Function 15 (ESF 15) External Affairs	05/08/2012	0.1
IS-00271	Anticipating Hazardous Weather & Community Risk	03/29/2012	1.0
IS-00271.a	Anticipating Hazardous Weather and Community Risk 2nd Edition	05/22/2015	0.9
IS-00293	Mission Assignment Overview	06/14/2011	0.3
IS-00315	CERT Supplemental Training: The Incident Command System	08/17/2013	0.3
IS-00317	Introduction to CERT	05/01/2017	0.6
IS-00346	Hazardous Materials for Medical Personnel	01/13/2012	1.0
IS-00360	Preparing for Mass Casualty Incidents: Guide for Schools, Higher Education, and Houses of Worship	07/25/2013	0.3
IS-00453	Introduction to Homeland Security Planning	05/01/2017	0.2
IS-00454	Fundamentals of Risk Management	05/01/2017	0.2
IS-00523	Resilient Accord - Exercising Continuity Plans for Cyber Incidents	10/12/2016	0.3
IS-00545	Reconstitution Planning Course	03/07/2018	0.4
IS-00546.a	Continuity of Operations (COOP) Awareness Course	12/16/2013	0.1
IS-00547.a	Introduction to Continuity of Operations	05/09/2011	0.2
IS-00548	Continuity of Operations (COOP) Manager	12/15/2013	0.4
IS-00660	Introduction to Public-Private Partnerships	12/20/2011	0.2
IS-00662	Improving Preparedness and Resilience through Public-Private Partnerships	04/17/2012	0.2
IS-00700	National Incident Management System (NIMS), An Introduction	10/17/2008	0.3
IS-00702.a	NIMS Public Information Systems	06/15/2010	0.3
IS-00703.a	NIMS Resource Management	06/16/2010	0.3
IS-00704	NIMS Communications and Information Management	08/28/2009	0.2
IS-00720	An Introduction to NET Guard	08/09/2012	0.1
IS-00775	EOC Management and Operations	05/25/2010	0.4
IS-00800.b	National Response Framework, An Introduction	10/18/2008	0.3
IS-00802	Emergency Support Function (ESF) #2 Communications	10/17/2008	0.0
IS-00805	Emergency Support Function (ESF) #5 Emergency Management	12/08/2009	0.0
IS-00806	Emergency Support Function (ESF) #6 Mass Care,Emerg. Assistance,Housing,Human Service	05/20/2011	0.0
IS-00808	Emergency Support Function (ESF) #8 Public Health and Medical Services	05/10/2011	0.0
IS-00809	Emergency Support Function (ESF) #9 Search and Rescue	05/20/2011	0.0
IS-00813	Emergency Support Function (ESF) #13 Public Safety and Security	02/13/2011	0.0
IS-00815	A-B-C's of Temporary Emergency Power	04/06/2017	0.2
IS-00860	Introduction to the National Infrastructure Protection Plan (NIPP)	10/17/2008	0.2
IS-00890.a	Introduction to Interagency Security Committee (ISC)	02/12/2011	0.1
IS-00906	Basic Workplace Security Awareness	04/06/2017	0.1
IS-00907	Active Shooter: What You Can Do	05/20/2011	0.1
IS-00908	Emergency Management for Senior Officials	04/05/2017	0.1
IS-00909	Community Preparedness Implementing Simple Activities for Everyone	01/05/2012	0.1
IS-00910	Emergency Management Preparedness Fundamentals	03/02/2012	0.3
IS-00913	Critical Infrastructure Protection: Achieving Results through Partnership and Collaboration	03/24/2013	0.2
IS-00913.a	Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration	04/10/2017	0.2
IS-00914	Surveillance Awareness: What You Can Do	04/06/2017	0.1
IS-00915	Protecting Critical Infrastructure Against Insider Threats	07/25/2013	0.1
IS-00916	Critical Infrastructure Security: Theft and Diversion - What You Can Do	07/25/2013	0.1
IS-00921	Implementing Critical Infrastructure Protection Programs	08/09/2012	0.3
IS-00921.a	Implementing Critical Infrastructure Security and Resilience	04/11/2017	0.3

Course Code and Title		Completed	IACET CEUs*
IS-00923	Performance Management-Goal Writing	04/05/2017	0.1
IS-01900	National Disaster Medical System (NDMS) Federal Coordinating Center Operations	03/16/2012	0.3
IS-02000	National Preparedness Goal and System Overview	06/20/2018	0.2
IS-02001	Threat and Hazard Identification and Risk Assessment (THIRA)	01/04/2014	0.1
IS-02002	Introduction to FEMA Operational Planning	06/19/2018	0.4
IS-02500	National Prevention Framework, An Introduction	06/12/2018	0.2
IS-02600	National Protection Framework, An Introduction	06/12/2018	0.3
IS-02700	National Mitigation Framework, An Introduction	06/12/2018	0.3
IS-02900	National Disaster Recovery Framework (NDRF) Overview	04/05/2017	0.2

**********End of Transcript**********

Tony Russell
Superintendent
Emergency Management Institute

*** One Continuing Education Unit (CEU) is equal to ten (10) student contact hours using the guidelines of the American National Standards Institute (ANSI) / International Association for Continuing Education and Training (IACET) I-2007 Standard.**

TRAIN ▪ SERVE ▪ RESPOND

TEXAS ENGINEERING EXTENSION SERVICE

The Texas A&M University System

IN COOPERATION WITH THE

DEPARTMENT OF HOMELAND SECURITY

FEDERAL EMERGENCY MANAGEMENT AGENCY

David G. Sweigert

has successfully completed

Threat & Risk Assessment Course

McClellan AFB, California

16 Hours

1.60 CEUs

April 11 - 12, 2012

Gary F. Sera, Director
Texas Engineering Extension Service

A. G. Davis, Director
Homeland Security Services
Texas Engineering Extension Service

TEEX
TRAIN ▪ SERVE ▪ RESPOND

TEXAS ENGINEERING EXTENSION SERVICE

The Texas A&M University System

IN COOPERATION WITH THE

DEPARTMENT OF HOMELAND SECURITY

FEDERAL EMERGENCY MANAGEMENT AGENCY

David G. Sweigert

has successfully completed

Enhanced Threat and Risk Assessment

San Francisco, California

16 Hours

1.60 CEUs

October 3 - 4, 2012

AUTHORIZED IACET PROVIDER

Gary F. Sera, Director
Texas Engineering Extension Service

A. G. Davis, Director
National Emergency Response Training Center
Texas Engineering Extension Service

TRAIN ▪ SERVE ▪ RESPOND

TEXAS ENGINEERING EXTENSION SERVICE

The Texas A&M University System

IN COOPERATION WITH THE

DEPARTMENT OF HOMELAND SECURITY

FEDERAL EMERGENCY MANAGEMENT AGENCY

David G. Sweigert

has successfully completed

Critical Infrastructure Key Resources Awareness Course

Mather, California

8 Hours

.80 CEUs

January 24, 2013

AUTHORIZED IACET PROVIDER

Gary F. Sera, Director
Texas Engineering Extension Service

A. G. Davis, Director
National Emergency Response Training Center
Texas Engineering Extension Service

State Board for Educator Certification #500132

EXHIBIT THREE

A study of the Port of Charleston evacuation and closure: How Live Action Role Play (LARP) Simulations create Cognitive Threat Vectors

June 2017

Dave Sweigert, M.Sci.

ABSTRACT

Examination of the Port of Charleston emergency evacuation and closure deliberately caused by anti-government social media "conspiracy theorists" is a harbinger of things to come. Role planning games that weaponize sensationalized "crowd-sourced" information represent a new emerging threat to critical infrastructure operators. Note: this paper is scholarly research and distributed for discussion purposes only.

Executive Summary

On June 15, 2017 two YouTube "conspiracy theorists", known as Jason Goodman and George Webb, created a sense of hysteria amongst LiveStream "crowd source" fans that the container ship Maersk Memphis was sailing into the Port of Charleston with a "dirty bomb" onboard.

These "online researchers" set events in motion that led to the evacuation of part of the port. A rigorous bomb sweep was conducted with nothing found.

The two apparently operate the web-site "CrowdSourceTheTruth", a Live Action Role Play (LARP) site, that seeks the help of fans to solve mysteries and conspiracy theories. The premise of this LARP is the distribution of "INTEL", in real-time, of information submitted by on-line fans. Webb/Goodman then form conclusions as to threats. The "threat" is broadcast to the LARP players with a soft inducement; a call to action is apparently inferred, and soon fans begin notifying authorities to warn of the threat.

Unfortunately, in the case of the Port of Charleston, dirty bomb warnings were received from multiple LARP players. Apparently, the intake of multiple sources of threat information demanded action, forcing the Port to be closed. Thankfully no was hurt during this bomb hoax.

Cognitive Threat Vector ("hack")

It is instructive to view the "crowdsource intelligence" and this LARP "fusion center game" in the context of cognitive threats to critical infrastructure.

A threat vector is a path or a tool that a threat actor uses to attack a target. Threat targets can be anything of value to the threat actors.

In this case it appears that participants within the LARP are lead to believe that actionable evidence exists of an urgent nature that requires action (e.g. notify Port Security of an incoming dirty bomb).

The "crowdsource" plot is advanced by the game controllers leading players to a call for action.

Potential for malicious use

This "fusion center game show" format purports to follow the process to source, validate and disseminate intelligence. This apparently legitimate process can be sensationalized by the game controllers to co-opt participants.

To be effective, LARP game controllers hold authority positions, such as reputable journalists or "internet researchers". Webb/Goodman are fond of telling their LARP players that they are "internet researchers conducting an independent investigation" of current topics (ranging from who killed Seth Rich to human trafficking).

Viewers appear to be specifically vulnerable to inclusive roleplay which simulates real time espionage efforts through mock clandestine scenarios produced on video for dissemination through various social media platforms.

This message then becomes cognitively invasive, working exponentially, per viewer, with each comment further forming a directed opinion, adding validation to a fabricated scenario.

The exponential contamination of LARP players grows, regardless of viewer opinion. Negative and positive opinions build further accreditation for fabricated clandestine acts as viewers clash.

A cognitive worm is created which appears based on "crowdsourced data". Debating amongst players, causes viral spread of cognitive worm, causing exponential viewers and mediums of dissemination. This eventually leads to player hysteria, angst or fear.

When critical mass is achieved and it appears the players have identified information requiring urgent action, then a call to action is inferred. Such calls to action could include botnet attacks, distributed denial of service (DDOS) attacks, public relations campaigns to disparage public officials, infrastructure operators, etc.

This type of threat vector can be added as an overlay to underlying cyber threats to create a multi-layer attack which critical infrastructure operators need to be aware of.

Urgent calls to action by unwitting players (port evacuation) can augment, amplify and mask other accompanying attacks. The fact that this new format of "crowdsourcing" represents a threat to owners and operators of critical infrastructure was clearly demonstrated in the case of the Port of Charleston.

Distribution of clandestine files

Two weeks prior to the Port of Charleston event, Webb/Goodman coordinated an on-line distribution of 1.1 Gb of files that they claimed were the property of the Democratic National Committee (DNC). The pair uploaded the files to a public document sharing site at the climax of two days of sensationalized on-line theatrical drama.

Then, in the early morning hours Webb/Goodman advised their audience it was crucial that they copy these files to their end-point computers to prevent forces working for the "deep state" from deleting these files.

Several hours after the mass download both Webb/Goodman announced that there was a possibility that beaconing malware may have been embedded in the files.

This is a troubling practice as the parties (Webb/Goodman) knew they were in possession of files they had no legitimate right to. Allegedly, these files contained Personal Identifiable Information (PII) of DNC donors; to include, names, home addresses, donations, etc.

These activities raises serious questions about LARP fans and devotees of Webb/Goodman that respond to their calls for action. This network, perhaps made up of unwitting participants, represents a type of cognitive botnet or DDOS-style attack ("beaconing" malware allegedly discovered after the mass download).

This demonstrates that with the right theatrical narrative, a network of LARP players can be induced into the potential commission of a federal or state crime.

Reputational damage to hospitals

Another disturbing tactic of this LARP style collaboration is the "investigation" into organ harvesting by American hospitals. Webb has distributed videos standing in front of hospitals while accusing the institution and staff of unethical organ transplants. In general terms, Webb classifies this under the category of "organ harvesting".

The potential for outraged LARP players to take action against such an institution should seem obvious.

"DOXing" of individuals

Another disturbing tactic used by the Webb/Goodman team is to reveal the PII of their enemies to their audience. Often times accompanied with a valid inducement that audience members should take some type of action against the dox'ed individual.

> Doxing is the Internet-based practice of researching and broadcasting private or identifiable information (especially PII) about an individual or organization.

Summary

The totality of activities undertaken by the Webb/Goodman team should be troubling to healthcare institutions and critical infrastructure operators.

These activities (distribution of unauthorized software, crowdsourcing threat information that resulted in the closure of a major port, DOX'ing of individuals and inflicting reputational damage on institutions) should be taken very seriously.

These activities represent the future of a new kind of threat. The emerging trend towards such cognitive attack vectors should be understood and prepared for. Planners should consider that in the case of a multi-layer attack, such "soft" cognitive attacks can be used to mask and distract security personnel.

About the author

Unfortunately, George Webb Sweigert is the author's brother.

EXHIBIT FOUR

Report: The Port of Charleston Dirty Bomb Hoax and Social Media Liability

by Dave Sweigert (Author)

★★☆☆☆ ▾ 15 customer reviews

› See all formats and editions

Paperback
$6.95

3 New from $6.95

The only report that has ever been written about the Port of Charleston, S.C. Dirty Bomb Hoax of June 14, 2017. This booklet describes how social media hoax news sites can attack America's critical infrastructure. Seemingly, these deception merchants operate with no threat of legal action. This fertile environment has allowed the consequence-free attacks on maritime ports, generation of hysteria of supposed assassination plots, and generate fear over unsafe consumer products. The next generation of

▾ Read more

Look inside ↓

See all 2 images

The Amazon Book Review
Author interviews, book reviews, editors picks, and more. Read it now