THE STRATEGIC NEWS SERVICE©

GLOBAL REPORT ON TECHNOLOGY AND THE ECONOMY™

SPECIAL LETTER:

IIOT: A CLEAR AND PRESENT DANGER

SNS Special Letter:
IIoT: A Clear and Present Danger

In This Issue

Week of 8/26/2019 Vol. 24 Issue 27

FiRe 2019™

On Our Agenda

ANTICIPATING THE UNEXPECTED

FiRe 2019 is all about helping you anticipate pivots, trends, and tipping points in an increasingly volatile and unexpected world.

How will the future of genetics and the climate crisis impact the global economy and the future of your business? How and when will general AI evolve? And what's the real story about the future of 5G? You'll find all of this – and more – at FiRe 2019, including:

China's Economic Strategy

- Kim Stanley Robinson, Science-Fiction Author
- Mark Anderson, Chair, Future in Review; Founding CEO, Pattern Computer Inc.

Teaching Cars to See: Sensor Tech in the Autonomous Industry

- J. Augusto de Oliveira, EVP & CTO, Cypress Semiconductor
- James Barrese, Strategic Advisor & Investor, Altos Group; Former CTO, PayPal

What the Federalism: The Election Machines Are Broken

- Harri Hursti, Founding Partner, Nordic Innovation Labs
- Jody Westby. CEO, Global Cyber Risk; Professional Blogger, *Forbes*

Reinventing Personal Health Through Circadian Rhythms

- Larry Smarr, Founding Director, Calit2 (a UCSD/UC-Irvine Partnership)
- Satchin Panda, Professor, Regulatory Biology Department, Salk Institute
- Pam Taub, Assoc. Professor of Medicine, Division of Cardiovascular Medicine, UCSD

Learn more about FiRe 2019 and see the latest agenda here.

Interested in having a presence for your company at FiRe? Remaining **partnership opportunitie**s for FiRe 2019 are available here. Contact SNS Director of Programs Berit Anderson at berit@stratnews.com to learn more.

FiRe 2019 Speaker Spotlight: Osh. Agabi on Computing with Lab-Grown Neurons

Nigeria-born **Osh.** [*Note:* period not a typo] **Agabi** has lived in six countries across three continents and speaks five languages. But that's far from the most impressive thing about him.

Osh. is the founder and CEO of Koniku, a company that combines lab-grown neurons with FPGA chips to create machines that can sense volatile organic compounds (VOCs). A form of chemical data both human-made and emitted by plants and animals, VOCs can be found in breath, the microbiome, and sweat glands, as well as urine and other bodily wastes. And Osh. is using Koniku's iPhone-sized sensing machines,

known as Konikores™, to identify trends that aren't currently trackable by traditional silicon chips alone.

Koniku has already landed customers in the aviation and pharmaceutical industries, including AstraZeneca, the UK-based pharma company. Boeing signed a letter of intent to use the tech in chemical-detecting drones. One customer, a drone company, hopes the processors will prove superior in detecting methane leaks in oil refineries. Another aims to use the processors to model the effect that certain drugs will have on a human brain.

In July, Koniku inked a long-term collaboration with Stuttgart's Fraunhofer Institute IPA, with funding from the Baden-Württemberg Ministry of Economic Affairs, to help build out manufacturing for Konikores and to establish the institute as a synthetic biology manufacturing base. We're delighted to welcome Osh. to Future in Review 2019 for a conversation about the future of computing.

Publisher's Note: There are times when a techno disaster is coming, everyone knows it, we all discuss it, and yet still it arrives. In the world of IIoT (Industrial Internet of Things) and critical infrastructure, that time was already a few years back.

As you'll see below, last week I had the pleasure of joining a panel on theCUBE, Silicon Angle's podcast series on this subject, together with well-known China IP-theft expert Evan Anderson and Phillip Lohaus, similarly qualified on the government side and now at the American Enterprise Institute. As I'm doing here, it seemed the right idea to switch the conversation early on from "What if," with regard to enemies in our infrastructure, to "What's next?" Anyone who thinks, given China, Russia, and the US (throw in Iran and NK for good measure) and their proven APT abilities, that all of us are not already embedded with logic bombs in all of our critical infrastructures, is just not paying attention.

If true, and I believe it is, then why hasn't anyone taken down a whole country yet?

The answer is simple: the knowledgeable experts on all sides fear this kind of "Cybergeddon" more than they fear a limited nuclear exchange. Why? Because the latter would be limited, with predictable death and destruction rates. The former would not.

In other words, we are now facing a new global security problem: in a world of infrastructure quickly dominated by machine-to-machine network communications, and with billions to trillions of completely insecure IIoT devices embedded therein – well, what could possibly go wrong?

In this week's issue, Jeff Hussey, CEO of Tempered Networks who earlier founded the amazing F5 Networks, talks about how to respond to this threat. To all of our members who use electricity, drink water, or want to sleep at night, I know you'll be interested in what he has shared with us in this week's discussion. – *mra.*

SPECIAL LETTER

IIOT: A CLEAR AND PRESENT DANGER

by Jeff Hussey

Two weeks ago, a former Wall Street infrastructure analyst named Gabe Lowy released a paper citing the critical risks of IIoT [Industrial Internet of Things] being ignored as organizations rush to exploit the substantial business benefits of digitalization. His paper, "Securing Critical Infrastructure Against Cyberattack," led to a theCUBE Power Panel recorded just days after its release: "IIoT and Cybersecurity: Apocalypse Now or Later":

Power Panel - IIOT: Apocalypse Now or Later, CUBE Conversation, August 2019

The problem exposed by the panel: the traditional network security stack deployed at virtually all organizations that care about network security is being rendered irrelevant by a growing attack surface of billions of insecure devices being connected to the internet at a dizzying pace.

[Lowy talks about the firewall problem in this 102-second clip from theCUBE.]

The Digital Advantage Powers IIoT Adoption and Increases Cyber Risk

The immense power of digitalization has given organizations massive operating gains and reset competitive battles and market share across a range of industries. Enhanced data collection and analysis, combined with agile response, has become a game changer. Yet the power resides in the secure network connecting the growing populations of computerized IIoT controls and devices, which control everything from factory floors to healthcare biomed devices and even maritime navigation systems.

> *"As more OT (operational technology) devices and industrial control systems (ICSs) are connected to IT […] systems over the Internet, the attack surface expands exponentially. Attackers can use search tools such as Shodan to identify vulnerable devices, which when breached, can cause catastrophic loss."* – Gabe Lowy, "Securing Critical Infrastructure Against Cyberattack"

Whoever controls those devices now owns the physical spaces those devices control. This is a fundamental shift in the power of the internet, because it represents a greater deal of accessibility and control of physical spaces, machines, and even smart appliances.

Losing control of data is painful. But losing control of a building or factory or hospital is on quite another scale. And yet it has already happened. Several recent IIoT cyber attacks (NotPetya, WannaCry) are among the most devastating ever, with victims including FedEx, Maersk Shipping, and hundreds of hospitals and clinics around the world.

Leading cybersecurity vendors were noticeably silent when those attacks targeting infrastructure in Ukraine easily spread globally through thousands of "protected" networks. Patching systems was the recommended countermeasure.

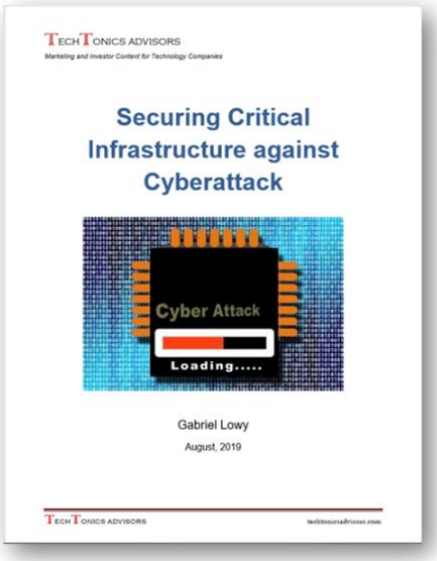
Ars Technica said it well:

> Last Friday, members of the Microsoft Security Response Team practically begged organizations that hadn't patched vulnerable machines to do so without delay, lest another WannaCry scenario play out. "It only takes one vulnerable computer connected to the internet to provide a potential gateway into these corporate networks, where advanced malware could spread, infecting computers across the enterprise," MSRC members wrote. In a rare move, officials with the National Security Agency on Tuesday echoed Microsoft's warning.

Many of these IIoT devices cannot be easily patched; nor were they designed with any kind of cybersecurity in mind. They had for years been deployed behind air gaps, where access could only be granted locally. Digitalization (IIoT) changes the game by changing the basic business and vulnerability potential of the internet, bridging the airgap with internet connectivity.

Firewalls Are DOA for IIoT

Lowy called out the growing gap between traditional network security architectures and the new demands of IIoT in his theCUBE interview. He also predicted a shift from network security solutions (such as firewalls) architected for traditional IT security demands (smaller networks, endpoints continuously updated / patched, etc.) to new solutions purpose-built specifically for IIoT.



Lowy also spoke specifically about the shortcomings of firewalls for IIoT. They were architected to protect far simpler north / south traffic into a network that had fewer connections to the internet. With IIoT you cannot place firewalls in between every internet access point for every device on a network. This critical, growing gap between the traditional firewall mission and the new network reality renders firewalls DOA for IIoT and sets the stage for a new security layer in an already complex stack.

Microsegmentation Complexity Doesn't Scale for IIoT

Microsegmentation solutions evolved to address many of the firewall management and cost issues as organizations struggled to deploy interior firewalls to isolate their "crown jewel" applications and data from access by bad actors, or what one analyst called the "internet cesspool." This worked to some extent, but it introduced even more complexity. More complexity meant more skilled staff were needed to simply protect the existing network before IIoT.

We at Tempered Networks have called this heightened complexity "stack fatigue," or the declining security posture which results as new solutions are added inside the existing layers of solutions already deployed. More complexity equals less security.

In short, we are seeing billions of insecure devices being attached to the internet at an increasing pace because businesses understand the payoffs of IIoT in terms of agility, intelligence, and operating efficiency. Yet all of the benefits of digitalization are offset by greater exposure to catastrophic risks, which has not been fully understood by business leaders racing into the digital age.

The net result is that our institutions are more vulnerable to the whims of bad actors than ever before. And this is no longer just about computer systems, but also the control of physical spaces, machinery, biomedical devices, ship navigation systems, and so forth.

"… [A]ll of the benefits of digitalization are offset by greater exposure to catastrophic risks, which has not been fully understood by business leaders racing into the digital age."

And even when it comes to bad actors, the stakes are higher than ever. NotPetya was a nation state-sponsored attack that inadvertently spread beyond the borders of its target. The implication is clear: we're all exposed in some way or another.

Bad Actors Include Nation-States

A week after the Power Panel talk described above, Mark Anderson and Evan Anderson appeared with Phil Lohaus to expose how dire the situation has become, especially within the context of IIoT and cyberwar. One of the takeaways: we've already been compromised. As the attack surface grows, these types of attacks will become even more destructive.

IIoT could very well become the new battleground, if it isn't already. Readers of recent SNS issues are well aware of the hostile intentions of several nations along with our growing interconnectivity.

This summer, a security advisory went out for vulnerabilities in VxWorks, an operating system in more than 2 billion IIoT devices worldwide, of which 200 million may be hard to patch. These devices were not built or installed with cybersecurity in mind, nor are their manufacturers cybersecurity experts. This is in

stark contrast to the evolution of PC, server, and smartphone security, with regular upgrades and product refresh cycles (the average IT network).

What's at Stake: Control

As both panels indicated, the cyber risks inherent with IIoT involve the physical control of spaces … the ability to change the direction of a ship at sea, shut down a power grid and/or a factory, or even force a hospital to cancel procedures and go back to using paper charts.

The lesson is clear. While IIoT is the future our digital age is being built on an insecure foundation beyond the scope of today's multibillion-network security industry. Many organizations are proceeding with IIoT strategies without viable solutions for critical issues, which is why we continue to witness major breaches and are warned to patch our systems.

I'm familiar with networking. In 1996 I founded a company called F5 Networks, at the beginning of the enterprise web era. My team saw how vital server load balancing was to the future of the internet and e-commerce. We helped organizations scale and secure their rapidly growing data centers.

Secure Networking Is the Foundation of the Connected World

Today, with our understanding of how critical secure networking is to the future of the connected world, the team at Tempered Networks has developed – with the help of a leading aerospace manufacturer and the military – an advanced architecture purpose-built for the unique security, resilience, scale, and management demands of IIoT.

We can protect the billions of IIoT devices without forklift upgrades to the already complex security stack or requiring advanced network security training for the new generation of cyber pros. I think Tempered has an even bigger role (than F5) this time by allowing organizations to scale IIoT faster with less security risk. We can make the digital world a safer, more productive place.

We can help organizations take full advantage of digitalization without having to accept growing security risks as a cost of doing business.

I'll be attending Future in Review in October in La Jolla, and I look forward to your thoughts as well. Let's work together to make the digital world one we all want to live in.

About Jeff Hussey

Jeff Hussey is the president and CEO of Tempered Networks, the pioneer of the identity-defined networking market.

As an accomplished entrepreneur and business leader with a proven track record in the networking and security markets, Jeff also founded F5 Networks, the global leader in application delivery and an S&P 500-listed company. He maintains numerous board positions across a variety of technology, nonprofit, and philanthropic organizations.

Currently, Jeff is the chairman of the board for Carena and chairman and co-owner of Ecofiltro and PuraVidaCreateGood. He also serves on the boards of Webaroo and the Seattle Symphony. He was the chairman of the board for Lockdown Networks, which was sold to McAfee in 2008.

Jeff received a BA in Finance from Seattle Pacific University and an MBA from the University of Washington.

I would like to thank Jeff for taking on this rather daunting task, and sharing his views with our members. To do a deeper dive, join Jeff and other security experts at FiRe 2019.

And, last and never least, our gratitude to Editor-in-Chief Sally Anderson, for putting all of these thoughts into perfect shape.

Your comments are always welcome.

Sincerely,

Mark R. Anderson

CEO
Strategic News Service LLC
PO Box 1969
Friday Harbor, WA 98250 USA

Tel.: 360-378-3431
Fax: 360-378-7041
Email: mark@stratnews.com

INSIDE SNS

Visit "Inside SNS" for:

- Photo galleries of FiRe and other SNS events
- FiRe videos
- SNS iNews®
- The SNS blog, "A Bright Fire"
- The SNS Media page
- SNS FiReFilms
- Subscription rates and permissions
- About SNS and About the Publisher

UPCOMING SNS EVENTS

FiRe2019™

We look forward to returning to our FiRe roots on the beautiful California coast, **October 8-11, 2019, at The Lodge at Torrey Pines in La Jolla**.

Join us for four days of industry-changing conversations, problem-solving with global leaders, lively debates, and social events, including an exclusive tour of UCSD's Calit2 Lab. And you'll connect with the world's most strategic thinkers and doers on tech, business, climate, and the global economy.

Registration is $5,900 and **includes complimentary three nights' stay*** at The Lodge, as well as all meals, social activities, program sessions, and networking events. ***Rooms must be booked by September 5** to assure this special lodgings offer!*

Our growing roster of 2019 speakers and moderators includes:

- **Paul Clayson,** CEO, Agile PQ
- **Andrea Crosta,** Executive Director, Earth League International (FiRe 2019 Featured Film, *Sea of Shadows*)
- **Thomas Aidan Curran,** CTO, Ory
- **Osh. Agabi,** Founder and CEO, Koniku Inc.
- **Susi Snyder,** Nobelist and President, ICAN

- **George Church**, Professor of Genetics, Harvard Medical School; Director, PersonalGenomes.org
- **Paul Jacobs,** CEO, XCOM
- **H.E. Ambassador Abraham Wen-Shang Chu,** Director General, Taipei Economic and Cultural Office in Los Angeles
- **Paul Maher,** General Manager, Microsoft
- **George Dyson**, Technology Historian & Nonfiction Author
- **Jack Gilbert,** Professor, UCSD School of Medicine and Scripps Institution of Oceanography; Group Leader for Microbial Ecology, Argonne National Laboratory
- **Bob Flores,** CEO, Applicology Inc., and former CTO, CIA
- **Harri Hursti,** Founding Partner and Hacker, Nordic Innovation Labs
- **Jeff Loucks,** Executive Director, Technology, Media, and Telecommunications Center, Deloitte
- **Ali Douraghy,** Chief Strategy Officer, Earth & Environmental Sciences, Berkeley Lab
- **Anne Hardy,** CSO, Join Digital Inc.
- **John Mattison,** Emeritus Asst. Medical Director and CMIO, Kaiser Permanente
- **Bill Hilf,** CEO, Vulcan Inc.
- **Don Norman,** Author and Founder, The Design Lab, Calit2
- **J. Augusto de Oliveira,** EVP & CTO, Cypress Semiconductor
- **Jody R. Westby,** CEO, Global Cyber Risk
- **Kim Stanley Robinson**, Hugo-Winning Author of Science Fiction
- **Maryanne Morrow,** CEO, 9th Gear Technologies Inc.
- **Steve Fey,** CEO, Totem Building Cybersecurity
- **David Gruber,** Presidential Professor of Biology, City University of New York / National Geographic Society
- **Pam Taub,** Founder and Director, Step Family Foundation Cardiovascular Rehabilitation and Wellness Center, Jacobs Medical Center, UCSD
- **Georg Kopetz,** CEO, TTTech Auto AG
- **Vanessa Pegueros,** Board Member, Carbon Black and BECU; former VP and CISO, DocuSign
- **Jason Schwartz,** CEO, Ecellix Inc.
- **Dmitri Alperovitch**, Co-Founder and CTO, CrowdStrike
- **Satchin Panda,** Professor, Regulatory Biology Laboratory, Salk Institute
- **Kimberly Prather,** Distinguished Chair in Atmospheric Chemistry, UCSD
- **David Brin,** Founder, Futures Unlimited; Sci-Fi Author & Physicist
- **Rob Knight,** Founding Director, Center for Microbiome Innovation; Professor, Pediatrics and Computer Science and Engineering, UCSD
- **David Ewing Duncan,** Author and Independent Correspondent; CEO, Arc Programs
- **John Wells,** Producer and Co-Host, "Cool Science Radio," KPCW (NPR Affiliate)
- **Larry Smarr,** Director, California Institute for Telecommunications and Information Technology (Calit2); Harry Gruber Professor of Engineering, UCSD
- **Kimberly Dozier**, Global Affairs Analyst, CNN; Contributor, The Daily Beast
- **Ed Butler,** Senior Correspondent, BBC
- **The Pattern Computer Team** (www.patterncomputer.com)

And more to come ---

Register Now!

WITH GREAT APPRECIATION TO:

Our Global Platinum and FiReFilms Partner:

Global Platinum Partner:

Global Silver Partners:

Silver Academic Partner:

Exhibitor:

And Focus Channel Partners:

... for their Partnership and Support of SNS events.

ADDITIONAL SUPPORTING ORGANIZATIONS

FiRe Event Partner:

FUTURIST

FiRe Academic Partner:

SCI www.sci.utah.edu

And a warm welcome to our first round of FiReStarter 2019 companies:

AGILEPQ

BioLogiQ Smart Solutions For A Sustainable World

ECELLIX BATTERY INNOVATIONS

cloudeo

TEMPERED NETWORKS

Where's Mark?

• On October 2-3, Mark will be keynoting the Department of Energy / Argonne National Lab AI XLab conference at the Drake Hotel in Chicago. • On October 8-11, he will be hosting the 17th annual Future in Review Conference, at The Lodge at Torrey Pines in La Jolla, California. To register now, go to: www.futureinreview.com. • On November 19-20, he will be speaking at the Info-Tech LIVE conference in Las Vegas.

ISSN 1093-8494