EXCLUSIVE

The Jester Speaks,

AND BOY, WHAT HE HAS TO SAY!

BY ANTHONY KIMERY, EXECUTIVE EDITOR

The Jester burst onto the scene in 2010 when he spectacularly began to take down jihadist recruiting websites. Since then, his notable targets have included nations that support, offer or grant asylum to Edward Snowden, the disgraced former National Security Agency (NSA) leaker of America's most classified sources and methods of foreign intelligence collection; Wikileaks — another purveyor of purloined US secrets — and the anarchist hacking collectives known as Anonymous, 4Chan, LulzSec and other hacker groups.

Conversely, The Jester's supporters say he's a "patriot hacker," a "grey hat hacktivist" and a "hacktivist for good." The Jester doesn't disagree, and actively cultivates this persona.

Laptop that was once used by The Jester to hack jihadist and terrorist websites on display at the International Spy Museum in Washington, DC.

PHOTO COURTESY OF THE INTERNATIONAL SPY MUSEUM

While federal authorities are very aware of The Jester's deeds, no known criminal charges have been pursued against him. It appears that all of the Internet Service Providers who've hosted the hundreds of websites The Jester has so far attacked reside outside the United States. For their part, Department of Justice and other government officials have declined to comment on whether they consider The Jester's actions to be criminal under US laws.

Meanwhile, The Jester's iconic characterization as a lone wolf hacker who plies his skills against forces beholden to evil ideology continues to grow among the legions who follow him on Twitter and regularly read his blog. And his followers include shadow operators in the US intelligence and counterterrorism communities. More than a few told *Homeland Security Today* on background that The Jester has, at the very least, their tacit approval. From the shadows, he's quietly applauded.

The Jester is believed to be a former member of the US military. He's repeatedly stated as much. After he has successfully attacked the target of his wrath, The Jester tweets out his now famous calling card, "TANGO DOWN," a military euphemism. A former Department of Defense official claimed The Jester was a former military contractor involved in US Special Operations Command projects. On April 10, 2012, The Jester gave a live chat interview to a class of computer science students at the University of Southern Maine during which he stated that he'd served in the military, completing four "operational tours."

In an interview with the website, threatchaos.com, The Jester claimed to have served as a former soldier in support of Special Forces deployed to Afghanistan. "I am an ex-soldier with a rather famous unit … I was involved with supporting Special Forces, I have served in (and around) Afghanistan amongst other places," he said.

Ashlee Vance, reporting in *The New York Times* on Dec. 3, 2010, quoted a Pentagon source as saying The Jester is "a former defense operative with knowledge of Special Forces activities" who "was a onetime military contractor who had worked on projects for Special Operations Command."

In his December 30, 2011 paper, "The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare," US Army cyber-operations specialist T. J. O'Connor "examine[d] the significant impact [this] lone-wolf patriot hacker has had over the course of the last two years, and what important lessons we can learn from him on how to wage a successful fight in this domain."

The paper "highlight[ed] the relatively successful patriot hacking campaign of The Jester."

"Largely motivated by his prior military service, The Jester appears focused on denying safe haven to terrorists and ministers of hate that use the Internet as their platform," O'Connor wrote. "In an early 2010 interview, The Jester discussed 'the horror of watching his friends and fellow soldiers be murdered by jihadi operatives who have long been exploiting the Internet.'"

The Jester has "argued that the omnipotence and growth of the Internet has granted terrorists a safe haven, and stated his intentions to prevent such action," O'Connor said. Furthermore, "The Jester claims to have discovered caches of jihadi information planted on legitimate US sites by jihadi hackers."

Continuing, O'Connor wrote that The Jester's desire "to deny Internet sanctuary to jihadists appears to stem from his military service. His service also appears to push his desire to protect both current and fallen American soldiers. … Over a two-year period, The Jester … successfully attacked over two hundred targets. One could argue that The Jester almost feels compelled to prevent his adversaries from succeeding in their message of hate. Considering the sheer enormity of targets The Jester has successfully attacked over a prolonged period of time, this endeavor has most likely become a lifestyle and mission for The Jester."

And that, The Jester said, he doesn't deny.

For several weeks in April up until a time that he was "stuck at a dodgy airfield waiting for [a] connecting flight," he engaged in a lengthy, exclusive interview with *Homeland Security Today*. He's rarely granted media interview requests. In this Q&A, which follows, The Jester explains why he does what he does, and offers his unique insights into the cyber-capabilities of Islamist jihadists and cybersecurity in general.

Q: Why do you do what you do?

A: For the green … and the girls, of course. No, seriously, both of those answers are wholly untrue, but I thought I'd try and break the ice a little. When I set about creating this online persona in 2010, it was purely to fill what I perceived was a void in our cybersecurity posture. The law regarding offensive cyber countermeasures was — and still is — a gray and murky area. So, instead of endlessly talking about what we might do, or what we could do, I decided as a private citizen to get up and just do it.

It's been a heck of a ride and in that time I've gained quite a following. It has been pointed out to me on many occasions that my moniker, "The Jester," is somewhat of a morale booster for our military downrange, and I'm in a position to actively support and promote the things that matter, like our troops, the Wounded Warrior Project and similar programs to assist our men and women in uniform.

And I also like to smite the bad guys. I guess that's why I continue to do what I do.

Q: What sorts of evolution have you seen from Islamist jihadists — and you've dealt with hardened Al Qaeda we'll kill you if we find you types — in response to your efforts to bring down their jihadi recruiting and radicalization websites? Are they getting smarter at thwarting and defending from the likes of you?

A: I've seen everything from low-tech obfuscation to some sophisticated codebase modifications to their web application of choice. It ranges from making the website appear to have been deleted when you hit the top level domain, to someone with programming knowledge crawling inside and changing everything about the site so that nothing is default — including directory structure and password hashing algorithms.

My original tactic was to continually knock *some* jihadi recruitment sites offline for limited periods of time while leaving others in place. This effectively, over time, caused them to become unable to trust their own systems, servers, abilities and service providers. The result was the jihadis gravitated towards the few top-tier sites I wasn't hitting. This created a 'funneling,' or 'herding effect,' that forced them into a smaller space on the Internet, and by definition, a smaller space is easier to watch.

Most of the jihadi sites I've hit were on shared hosting packages, meaning they share a server with other clients. Many of the providers got sick of their shared boxes being downed as it adversely affected other clients, and therefore business, and so the hosts cancelled or suspended the jihadi accounts.

Now, over the last year, there has been a marked uptick in Islamic fundamentalists shifting from trying to keep their own sites and servers up, and instead they are moving, sometimes exclusively, into social media such as Twitter and Facebook. These are all US companies with US servers. The offenders are often not US citizens, therefore I would assume their presence on these services is now even easier to monitor.

Q: How do you describe their skill levels against yours and the counterterrorism community?

A: For the most part, all but the top tier jihadi forums seem to be run and maintained by random sympathizers with little or none of the funding or skills required to keep a website or forum up and running. With that said, however, the high value forums like As Ansar and Al Shamukh for example, seem to be operated by coders with some degree of skill in PHP and database management, as well as server hardening techniques. These are the places where the real hardcore fanatical fundamentalists like to hang out. They monitor who is coming and going and you are not getting into these forums as a regular user without being vouched for by other members. That being said, I would imagine we have "inserted" TLA operators onto these forums by means of long-term social engineering in order to keep tabs on the bad guys within.

Q: What types of reprisals have Islamist jihadists and others tried to wage against you?

A: To my knowledge so far, from the Islamist fundamentalist corner, there have been a lot of threats, tantrums and shouting about "Jester," but nothing really scary. I have been made aware of two supposed fatwas — one dedicated to me and another against "American anti-Islam website administrators." My most effective weapon in fatwa avoidance is to maintain operation security and personal security at all times. Misdirection is also a useful tool in the box. It's one thing to bring down jihadi forums, but a whole different animal to do it for almost five years without getting sprung. I'm sure if my anonymity was blown, my family, friends and I would have a lot more to worry about with respect to personal safety.

One of the most annoying aspects of being the "Jester" is that, as time has gone by, a small persistent core of individuals see the prospect of outing my identity as a trophy prize that will further their own personal ambitions. They spend an unhealthy amount of time crawling up my flagpole and that of my followers trying to find a bead on who I am. They have even outright claimed that some of my Twitter followers are in fact me, and this is always a worry to me because all it takes is one crazy homegrown self-radicalized lunatic to buy into these crazy and wholly irresponsible theories and something very bad is going to happen to an innocent bystander.

I will say that the single most unsettling threat I have received to date was from Ms. Shirley Phelps of Westboro Baptist Church. She appeared on the David Pakman Show after I knocked out all of their domains for eight weeks and stated publically, and I quote: "If I could just find this guy who's called Jester, I would give him a big hug. I might even give him a little kiss on the top of his head."

That sent shudders down my spine, no doubt.

Q: Do you believe you get at least tacit support from our counterterrorism and intelligence agencies?

A: That is an interesting question, and one I get asked all the time. A part of me wants to believe the authorities are aware and turn a blind eye to my "activities," while at the same time another part of me hopes I haven't even popped their radar. However, the latter scenario is highly unlikely at this stage of the game. While I have no official relationship with any agencies and nobody tasks me or sends me directives on what to hit, I have, in the past, had messages come through from "other connected researchers" requesting that I not launch an attack against certain sites for a while.

Obviously, I comply, as nobody wants to be the guy who screwed up another long-term operation. With regard to why — to my knowledge at least — I am not part of an active investigation, I can only assume it comes down to the fact that my targets fall in line with what are widely accepted to be 'bad actors'. Also, to date, none of the jihadis or other bad actors I've targeted have rolled up to the FBI to file a complaint. The servers and services I attack are largely based outside of the US, which is a helpful situation for me ... not so much for them.

So far, I am still the ghost of John Doe.

Q: What do you recommend for the counterterrorism, intelligence and cybersecurity communities, based on your experiences?

A: While it's true that social media is used for bad purposes by the nefarious, it can also be harnessed for good. Take the Boston bombing, for example. In the immediate aftermath, there were literally thousands of photos being taken by members of the public on the ground and uploaded in real-time to places like Twitter. I have no doubt that these images served as an instant and accurate resource for authorities to analyze and narrow down the search for the perpetrators.

In the hours and days after the event, I myself started to look at the connections and conversations online between the Tsarnaev brothers and their friends. I documented my research on my blog. And now, a year later, some of the very friends of the Tsarnaevs I

The Jester on Snowden, Wikileaks and Brokering Secrets

BY THE JESTER

What we essentially have in Edward Snowden is a low-level private contractor who has lied about numerous things and embellished others since identifying himself. What we do know is he fancied himself as a bit of a ladies man, an "international man of mystery." A simple search of his Internet handle, "*TheTrueHOOHA*," pre-2013 reveals a very narcissistic character, although I am sure now he has a new found understanding as to why secrets are essential, considering he is hiding like a frightened puppy.

On whether Snowden was a premeditated spy working for the Chinese or Russians, I don't think this is the case, even though since fleeing there's no doubt in my mind that both these nations' respective intelligence services have gained access to the documents he fled with. That's not to say he wasn't a spy for someone else though, a middle-man if you like. In fact, Snowden himself admitted to the *South China Morning Post* that he "secured a job with a US government contractor for one reason alone — to obtain evidence of Washington's cyberspying networks."

Wikileaks, and specifically Julian Assange, are the brokers here, and it's not the first time Assange has targeted young individuals within our military and intelligence communities.

Much like Bradley "Chelsea" Manning, or whatever he's calling himself today, Edward Snowden was a person desperate to be somebody; they were both in trusted positions and both had an online presence (as most young people do), except these were guys in positions to provide information to Wikileaks. I believe, that much like pedophiles groom vulnerable or susceptible children online, so Assange grooms US personnel.

He didn't have to do it this way. Any rules regarding government employees — especially National Security Agency (NSA) — not being permitted to blow whistles; he didn't work for NSA. He worked for a civilian contractor. Another thing people are questioning is how he had access to this information. Well he didn't, and he wasn't a hacker either. What he did, as reported in *Newsweek*, was steal and or fabricate digital keys that gave him access to areas he was not allowed to visit as a low-level contractor. He was a common thief.

What was playing out with Snowden was a game of highest bidder, and Assange was the broker, and has been from the start. Remember Wikileak's staff, including Assanges' own girlfriend, Sarah Harrison, were on the scene in Hong Kong to hook up with Snowden simultaneously as he arrived. It's no coincidence.

Essentially, the puppet masters are Julian Assange and his "organization." To my mind, they represent the single biggest threat to our national security right now. They are clearly and actively seeking to "recruit" US personnel for the purpose of revealing US secrets. At the very least, this is designed to undermine the US around the world. At worst, it's a direct attempt to obtain and exchange with enemy nations our sensitive information — information that could feasibly put US assets downrange at risk, or give other nations a tactical advantage or insight into our operations.

picked out as complicit early on are currently being pursued as persons of interest.

I think that social media open-source intelligence (OSINT) crowd-sourcing should be embraced and developed by law enforcement agencies into something less chaotic and more cohesive, especially when major incidents occur. There are some excellent tools that any citizen can employ to assist in OSINT collection like Recorded Future, Maltego, Casefile, Tineye and many others.

Q: How do you see the future of cybersecurity evolving in the context of the sort of offensive cyber warfare you engage in?

A: Looking to the future, more recently I have been diversifying my cybersecurity interests. You kind of have to, as the threat landscape is constantly changing, too. I think the future is going to be all about the ongoing threat from the likes of China, Iran and their allies. China has some very questionable alliances and an entire People's Liberation Army [PLA] military unit called "61398" dedicated to attacking US cyber assets and pursuing, amongst other things, the direct theft of Western intellectual property.

[**Editor's note:** The reputed Shanghai-based unit of the People's Liberation Army General Staff Department known as Unit 61398 is said by Western intelligence to be the PLA's elite cyber-warfare agency, populated by perhaps thousands of China's best and brightest network security, digital signal processing and covert communications engineers.]

As we move forward, I think there also will be a heavy shift towards supervisory control and data acquisition (SCADA) security. SCADA systems are directly responsible for industrial processes, power generation, water treatment and much more, and many SCADA systems are directly connected to the Internet. These systems are easily found using tools like Shodan. An attacker who knows of a SCADA vulnerability ahead of time can look for susceptible systems and filter by country — or even company name, thus cutting down his target ing package research time hugely.

It's scary how easy it is.

This cuts both ways, though. We went into Iraq looking for WMDs, and this cost us lives, money and political face. Fast forward to the now, and there are capabilities such as "Stuxnet" and "Flame" floating around. The nature of Stuxnet was that it was a widely spread self-replicating virus or malware that most likely infected a great deal of personal and business computers, yet it had a specific payload that only triggered if specific conditions were met. Anyone not meeting these conditions was unaffected. However, if the malware detected itself was resident on a system inside Iran, and that system was running a certain piece of Siemens SCADA software that is exclusively used in nuclear plants, Stuxnet came to life and sabotaged the facility. This effectively allowed the attacker to switch off and or at least set-back Iran's nuclear weapons program without a single military boot on the ground.

Imagine the lives and money saved if we had deployed a similar capability back in Iraq.

Lastly, there is the evolution of online technology in our daily lives. The so-called Internet of Things, which basically connects devices that are not traditionally web-enabled, like cars, homes and fridges to the Internet. While this is definitely progress, it makes for an even more target-rich environment, and I believe attacks between nation states on these new emerging vectors is going to become much more prevalent. It will certainly open all kinds of new possibilities for espionage, both state-sanctioned and otherwise.

So keep your eyes peeled, and stay frosty. **HST**

Contributing Writer Matt Hoey contributed to this report.