YOU WERE WARNED: CYBERSECURITY EXPERT EDITION — NOW WITH SPACE STATIONS

Over the last handful of days breathless reports may have crossed your media streams about Stuxnet infecting the International Space Station.

The reports were conflations or misinterpretations of cybersecurity expert Eugene Kaspersky's recent comments before the Australian Press Club in Canberra. Here's an excerpt from his remarks, which you can enjoy in full in the video embedded above:

> *[26:03] "…[government] departments which are responsible for the national security for national defense, they're scared to death. They don't know what to do. They do understand the scenarios. They do understand it is possible to shut down power plants, power grids, space stations. They don't know what to do. Uh, departments which are responsible for offense, they see it as an opportunity. They don't understand that in cyberspace, everything you do is [a] boomerang. It will get back to you.*
>
> *[26:39] Stuxnet, which was, I don't know, if you believe American media, it was written, it was developed by American and Israel secret services, Stuxnet, against Iran to damage Iranian nuclear program. How many computers, how many enterprises were hit by Stuxnet in the United States, do you know? I don't know, but many.*
>
> *Last year for example, Chevron, they agreed that they were badly infected by Stuxnet. A friend of mine, work in Russian nuclear power plant, once during this Stuxnet time, sent a message that their nuclear plant*

> *network, which is disconnected from the internet, in Russia there's all that this [cutting gestures, garbled], so the man sent the message that their internal network is badly infected with Stuxnet.*
>
> *[27:50] Unfortunately these people who are responsible for offensive technologies, they recognize cyber weapons as an opportunity. And a third category of the politicians of the government, they don't care. So there are three types of people: scared to death, opportunity, don't care."*

He didn't actually say the ISS was infected with Stuxnet; he only suggested it's possible Stuxnet could infect devices on board. Malware infection has happened before when a Russian astronaut brought an infected device used on WinXP machines with her to the station.

But the Chevron example is accurate, and we'll have to take the anecdote about a Russian nuclear power plant as fact. We don't know how many facilities here in the U.S. or abroad have been infected and negatively impacted as only Chevron to date has openly admitted exposure. It's not a stretch to assume Stuxnet could exist in every manner of facility using SCADA equipment combined with Windows PCs; even the air-gapped Russian nuclear plant, cut off from the internet as Kaspersky indicates, was infected.

The only thing that may have kept Stuxnet from inflicting damage upon infection is the specificity of the encrypted payload contained in the versions released in order to take out Iran's Natanz nuclear facility. Were the payload(s) injected with modified code to adapt to their host environs, there surely would have been more obvious enterprise disruptions.

In other words, Stuxnet remains a ticking time bomb threatening energy and manufacturing production at a minimum, and other systems like those of the ISS at worst case.

As Kaspersky noted, there are three government

reactions to Stuxnet's continued proliferation in the digital world. The computing cowboys who likely approved, supported, created, and launched this cyber weapon continue their optimistic stance with regard to the use of cyber weapons.

The politicians who knowingly or unknowingly signed off on these weapons remain indifferent and clueless. (Hello, Congress?)

And the remainder are still terrified – *scared to death*, said Kaspersky – of the potential for a disaster set in motion by Stuxnet. They may have limited solutions, but funding could be dependent on people in the indifferent/clueless politician category. They may not have solutions, thwarted by the cyber warfare zealots in the first category, or by the nature of the technology itself (you'll notice Microsoft is doing nothing out of the ordinary about its vulnerabilities apart from offering a bounty to citizen bug hunters).

This does not sound like a formula for effective pre-emption of cyber weapons, does it?

We can only wonder what it will take for a critical mass of those persons responsible for effecting national security to get on the same page. Will it take more corporations the size of Chevron admitting to Stuxnet-infections?

Or will it take ISS breaking up spectacularly like an IMAX 3D-screened sci-fi movie before they catch a clue?

Whatever it takes, you know the responsible folks been warned – again, and again, and again.

You'll also recall the Stuxnet payload delivery method requires two different failures of security before it launches its payload: a fake or stolen security certificate, and encryption which unpacks the content. Neither of these challenges have been addressed effectively by the global IT community. The latter challenge may have been enabled in no small part by the National Security Agency's efforts to weaken of

National Institute of Standards and Technology’s encryption standards, used on Microsoft Windows devices – as discussed here in September. We’re still waiting for credible traction on this, as are members of the cybersecurity community.