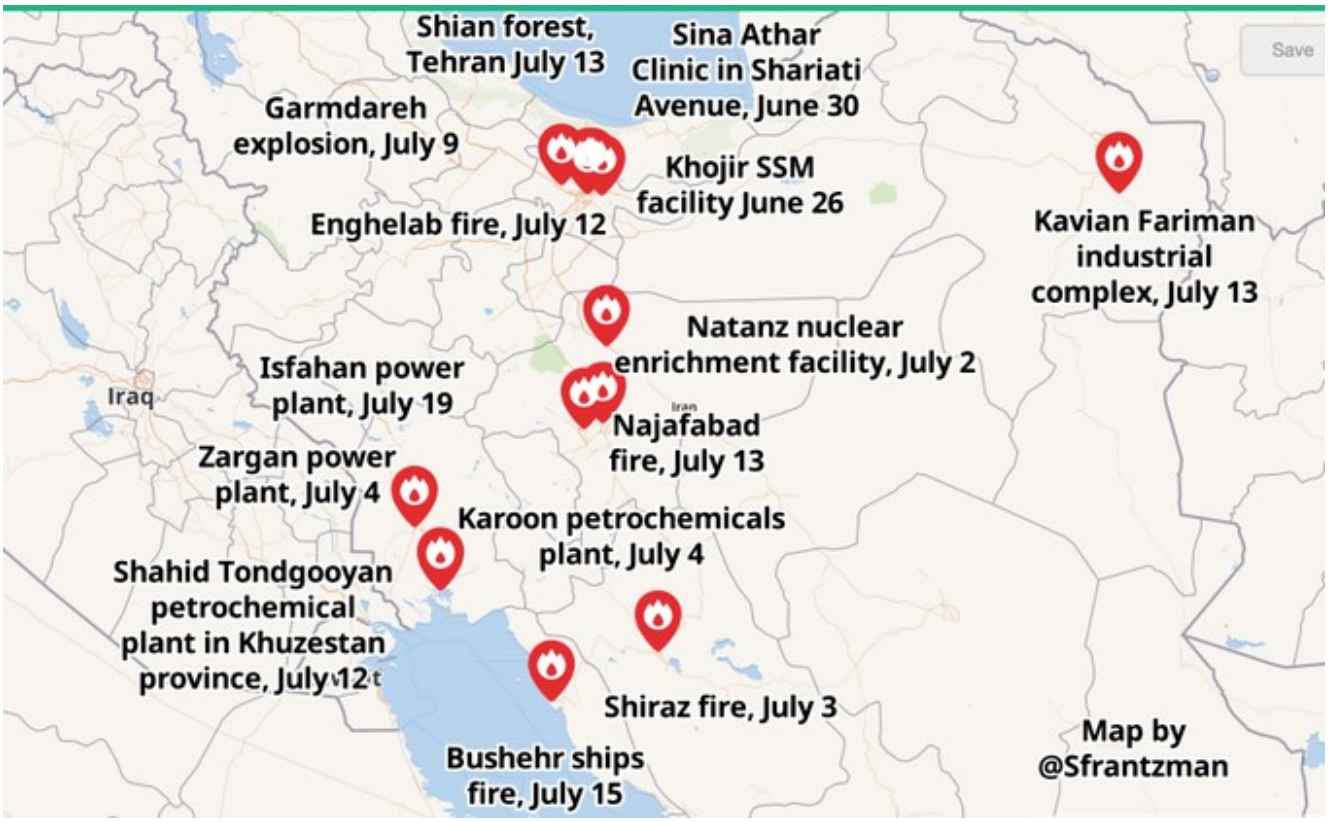
Iran's Nuclear Program Under Intense Pressure

An Interview with Dr. Stephen Bryen

by Jerry Gordon and Rod Reuven Dovid Bryant (August 2020)



Locations of fires and explosions in Iran through July 19, 2020, by Seth Franzman for *J Post*

The Middle East is witnessing a new form of kinetic cyber warfare that has dramatically set back Iran's nuclear program. Dr. Stephen Bryen, former Reagan era Deputy Under Secretary of Defense for Technology and Security, noted military technologist and *Asia Times* columnist calls it "Son of Stuxnet". That is a reference to the joint US-Israel malworm virus attack in 2009-2010 on the Natanz enriched uranium

cascade facility that destroyed an estimated 1,000 of 5,000 centrifuges. The difference this time was the cyber-attacks may have generated explosions.

Natanz was hit on July 2, 2020 by an explosion that destroyed the equipment and facilities for producing the current generation of advanced centrifuges. That according to David Albright of the Washington, DC-based Institute for Science and International Security (ISIS) may have set back Iran's nuclear weapons development by 2 plus years and even longer.

Bryen said that this round of cyber kinetic warfare was initiated when Iran cyberattacked Israel's water supply system on April 24 and 25, 2020. The water facility attack was intended to release large amounts of poisonous chlorine into Israel's water delivery infrastructure, potentially poisoning tens of thousands of Israelis. Israel responded by temporarily disabled the Iranian Shahid Rajaee port (Bandar Abbas) in the Straits of Hormuz.

More explosive events followed in late June and the first three weeks of July. Bryen noted some of these events:

• On June 26, a building in the solid fuel assembly plant of the Khojir Missile facility, which also deals with nuclear warhead designs, exploded with such force that it was seen 70 Kms. away. At the same time, an explosion and fire destroyed the power plant servicing the city of Shiraz, plunging it into darkness.

• On June 30, explosions ripped through the sub-basement levels of the Sina medical center in Tehran killing 19.

• On July 2, an explosion, claimed by an unknown opposition group, the Panthers of the Nation, ripped apart the new centrifuge assembly building in the Natanz nuclear center. The Iranian regime has all but admitted this is a major setback to its enrichment program. The same night, a

major complex exploded and burned in Shiraz.

• On July 3, an enormous fire erupted in the northwest part of Shiraz in an unknown location and facility. The same night, another large fire destroyed an unknown facility in Salmas near Tehran.

• On July 4, a fire and explosion in southwest Iran in the predominantly Sunni Arab province of Ahvaz destroyed the power plant. At about the same time, the Karoun Petrochemical plant failed and released what was claimed to be chlorine gas sending about six dozen to the hospital.

• Early on July 7, a powerful explosion engulfed a warehouse or factory of unknown use in Beqarshahr south of Tehran. This is the same vicinity in which the Israelis two years ago seized Iran's nuclear archives, namely Turouzabad- Kahrizak, and in which Israel and the IAEA suspect also was a major nuclear warehouse.

Bryen said the most significant cyber kinetic attack was against the Natanz centrifuge production facility. That was borne out in the post attack damage assessment made by ISIS. It concluded: "Although the explosion and fire at the Iran Centrifuge Assembly Center does not eliminate Iran's ability to deploy advanced centrifuges, its destruction must be viewed as a major setback to Iran's ability to deploy advanced centrifuges on a mass scale for years to come. "This was a crown jewel of their program," Albright of ISIS said in an interview with Eli Lake.

The implications are significant. Note what renowned Middle East Expert David Wurmser said in a *Bloomberg* article by Eli Lake: "The more Iran's government looks impotent, and the impression is left the Israelis are everywhere, the more high-level Iranian officials will calibrate their survival by cooperating with Americans or Israelis, which itself creates

an intelligence bonanza".

Here are some of the takeaways from the Bryen interview.

Vulnerability of Israeli and US Critical Infrastructure.

US and Israeli water, power, petroleum and gas processing, and manufacturing systems rely on the use of the (Supervisory Control and Data Acquisition) SCADA systems which are vulnerable to cyber-attack.
In 2016, Iran cyber warriors attacked controls on a water dam reservoir in suburban Westchester County, New York. Attacks on the national electrical grid in California in 2014 demonstrated its susceptibility to terrorist and cyber-attacks. Bryen said these attacks by a state sponsor of terrorism could be a "causus belli".

Importance of Plausible deniability in Cyber Warfare.

Bryen suggests that Israel has been "brilliant" in conducting sophisticated covert and cyber kinetic operations by using in-country assets and highly trained commandos to set up 'sleeper' explosions. This was amplified in remarks by former Vice Chief of Staff and Fox News Analyst General Jack Keane: "Keane thought the alleged strikes were 'a smart strategy' on the part of Israel. If you accept the objective that we don't want Iran to have nuclear weapons with missiles that can deliver them, then the strategy the Israelis are doing, likely with at least the moral support of the US, is fairly savvy because it gives the Israelis deniability," he explained.

The Footprints of Israel in the original Stuxnet.

The 2009-2010 Stuxnet malworm virus, Bryen noted, was imported into the Natanz facility, and spread by "Bluetooth" infecting the Siemens PCS-7 SCADA and programmable controllers that spun the centrifuges out of control. In the encrypted

code of Stuxnet was the term ‘My RTUs” meaning Myrtle- the Hebrew for Hadassah or Esther. There was also the code that triggered the spinning of centrifuges out of control: 19790509. That was the date of the execution of the leader of the Iranian Jewish community, Habib Elghanian, the head of the Tehran Persian Jewish Community. His death started the large wave of Iranian Jewish immigration.

Also discussed in the Bryen interview was the parallel launch of the Israeli Ofek16 satellite with more powerful cameras and sensors to provide intelligence on Iranian and proxy threats in the region. Bryen noted the success of an Alaska test of the Israeli Arrow ABM system able to attack ICBMs during launch phase which he gave a “B+” rating versus an F minus for the US Ground Based Mid-Course Interceptors.

What follows is the Israel Talk News Radio – Beyond the Matrix interview with Dr. Stephen Bryen.

Rod Bryant: Jerry Gordon and I have a fantastic show lined up for you. We have a guest that we have had on many times before, Stephen Bryen.

Jerry Gordon: Stephen Bryen is a brilliant military technologist, a former Deputy Under Secretary of Defense for Security and Technology. He has thoughtfully expressed his views in his Asia Times columns on a wide range of topics. This program has a bottom line: whoever perpetrated this sophisticated Son of Stuxnet cyber sleeper attack on facilities in Iran probably may have set back their nuclear program somewhere between two to five years.

Rod Bryant: We will explore the idea of how far behind many other countries including the United States, are in their capability of doing what Israel potentially may have done. We have a great show lined up for you with Stephen Bryen, me, and Jerry Gordon.

We are receiving an update on what went on with the bombing of

a facility or sabotage of several facilities in Iran, most prominently the nuclear facility at Natanz. Stephen, it is a real honor to have you back, a man of great knowledge and ability to analyze. We have received some particularly good comments from our listener audience that say you are really doing a great job providing some important analysis. Steve There were multiple cyber and sabotage attacks on Iranian nuclear facility, missile facilities. Please give us an update on what has happened.

Stephen Bryen: That is thanks to David Wurmser who has been keeping track of this. Dr. Wurmser, was in the NSC and an advisor to the Vice President. He is a real expert on the Middle East. Here is the run down on these kinetic attacks. The first one we know of was on June 26, 2020 that hit Khojir. Khojir is a missile manufacturing and production site. However, I have a suspicion that it is more than that doing things that relate to that involve nuclear weapons development. Specifically, I imagine they are working on a warhead. In any case, that was attributable by Iran as a gas explosion.

Rod Bryant: The reason why you are giving that analysis is why would they waste time on a normal missile facility, correct?

Stephen Bryen: Missiles are a real problem for Israel, the United States, and other countries. It is not trivial. We really do not know what they were about yet. But clearly, I think that if you are going to do it and it is urgent that you do it, there must be something going on that would trigger that target. I think that the Israeli intelligence is extremely good on this. I do not think there is much they do not know about. They never shared it with me, but logic says, there was something nuclear going on there.

Rod Bryant: They could have done this at any time, why now? Do you think that they had some intel that they were close to providing something that was nearing operational status?

Stephen Bryen: No, I think part of this is the fact that the Iranians are in high gear to produce nuclear weapons now. They have made no secret about it. They have been clear that is what they are doing producing highly enriched uranium and nuclear weapons delivery systems. It looks to me like this became an urgent matter. This was not something that happened on the spur of the moment. This was a very elegant, sophisticated series of assaults, rather than attacks. We do not know yet a whole lot about how it was done.

Rod Bryant: Do we know exactly how it was laid out or how these assaults happened?

Stephen Bryen: On June 30, there was a set of explosions underground underneath the Sina Medical Center in Tehran. Nobody knows exactly what was going on there either. However, you do not bomb medical centers. Obviously, what was underneath the medical center was all important. Probably, I think, there is a nuclear command center down there. On July 2, 2020, an unknown opposition group called Panthers of the Nation hit the Natanz Nuclear Center. This is huge. This is where Iran was developing and manufacturing advanced centrifuges building the rotors for all its centrifuges. It is a major facility. Three-quarters of which was destroyed, perhaps more.

Rod Bryant: That is big.

Stephen Bryen: Yes, it is a big operation. On July 3, 2020, there was an enormous fire in Shiraz. Shiraz is a lovely town, I visited it before the Iranian Revolution. No one knows exactly where, and no one knows what kind of facility it was, but everyone saw the fire. On July 4, 2020, our Independence Day, there was a fire in the southwest of Iran, mostly in Ahvaz that destroyed a power plant. On the same day, another petrochemical plant blew up. On July 7, 2020, there was a powerful explosion that took out a warehouse or a factory, south of Tehran. This is the same area where the Israelis

exfiltrated the Iran nuclear archives from a warehouse that they brought back to Israel.

Rod Bryant: Interesting.

Stephen Bryen: Does that tell us anything? It probably tells us there was a lot of activities going on right around these targets, those are the main explosions that have taken place. These assaults hit power plants, missile development and centrifuge facilities. We had a secret research or command facility buried underneath a medical facility in Tehran. The assaults appeared very systematic. Whoever carried out these systematic assaults with inept responses by Iran had compelling intelligence. The question is why? I think there are a couple of explanations. We cannot forget that earlier, the Iranian cyber echelons tried to damage the Israeli national water supply system in late April 2020. They hit six Israeli water facilities. All water supplies use chlorine as a disinfectant but in microscopic amounts, but they have tanks of liquid chlorine. They tried to release that into the water supply. If people drank that water or swam in that water, they would probably get extremely sick, if not die. Israel regarded that as an existential attack.

Rod Bryant: Was what they did successful?

Stephen Bryen: It was partially successful in the sense that these water supply systems had to be shut down. Some of the equipment was severely damaged. It was not successful in that the chlorine did not get into the water supply.

Rod Bryant: Now were they ever able to make any arrests? Was it an inside paid job? What do you think was going on with that cyber-attack?

Stephen Bryen: There have been no arrests, as far as I know. I think it was an external job, not an inside job. I think the cyber defenses, if you want to call them that, at these water facilities was below grade, let us call it poor. This is very

typical though, not only in Israel, but it is typical in the United States. We have a big critical infrastructure problem protecting water supply, food supply and …

Rod Bryant:—the Electrical grid system too.

Stephen Bryen: Electrical, petrochemical, transportation it goes on and on. The US critical infrastructure systems are very vulnerable. Almost all of them depend on industrial controllers, which are commercial items. They are called SCADA – the acronym for supervisory controlled data acquisition systems. The SCADA systems are vulnerable to attack through electronic or cyber means.

Jerry Gordon: In 2016, we had an event here in the United States, in Westchester County, New York that was attributed to Iranian cyber warriors, taking control of the water reservoir system for the county. We have also had other instances in this country, the most notorious one were the failures of water filtration systems in Toledo, Ohio in 2014 and Milwaukee, Wisconsin in 2017. The run-off of nitrates in Lake Michigan essentially resulted in microscopic toxic algae blooms. The worst example was the 1993 Milwaukee Cryptosporidiosis outbreak that resulted in the deaths over one hundred people. That underlines what Steven is talking about. We are not prepared in the United States to deal with protection of these important infrastructures essentially against foreign cyber-attacks.

Rod Bryant: We also understand that this is not isolated, that they have been doing this in other countries as well as the United States. We were talking about Iran and the recent sabotage work that has taken place in Iran, cyber-attacks, and bombings.

Steven Bryen: I would say, explosions. Because we are not sure. No one has come forward and told us it was a bomb.

Rod Bryant: They say it may have been gas leaks, Stephen,

Jerry brought up the idea that these are not isolated attacks that we have seen in Israel with Iranian cyber assault on their water system. We have we have seen it in the United States and other countries.

Stephen Bryen: Jerry was exactly right. There have been a lot of attempted attacks or practice attacks, on US critical infrastructure, targets, especially power plants, water supply and chemical facilities. The reason they are practicing is if they do it and it happens, it is a causus belli, or cause of war. The Iranians are just testing what they can get away with, trying to figure out how vulnerable we are. Unfortunately, we are vulnerable. Because virtually all manufacturing plants in the United States, and everywhere else in the world for that matter, use commercial SCADA systems. These are essentially supervisory control systems that manage how a factory operates. They control everything. They are basically a computer with special programming. They are susceptible to a cyber-attack where you can stop a factory from operating, cause the factory to make mistakes. You can do all kinds of things that are dangerous.

Jerry Gordon: Stephen, how close is Iran to producing enough fissile material for nukes?

Stephen Bryen: That is a particularly good question. No one knows the answer exactly. They have been refining uranium, but at the low end of the scale. To have enriched uranium sufficient for an atomic weapon, which is what I think they are aiming at, you need 95-98% enriched uranium. There are different ways to do it. If we talk about centrifuges, the first step is to reach the lowest level of enrichment, which is perhaps 10 or 15%. If you achieve that then you can move to the next step. That is through what the Iranians had in Natanz- cascades of centrifuges.

Rod Bryant: What is the process?

Stephen Bryen: It is a process of slowly extracting U-235 from the other compounds of uranium, largely U-238, but there are other parts in there too. This process has several steps. During World War II, when we first did that at Oakridge, Tennessee where we had a huge complex. We did not use centrifuges then, we used calutrons, which are essentially cyclotrons that spin the gas, and then they have scoopers pick up the different fragments or fractions. The highest fraction is U-235. That is what they want to skim off. However, you cannot skim it off pure. You skim off a little more of it than you would have had in the original. Then you use the gas to free those calutrons called uranium hexafluoride. Centrifuges work in a similar way. You have a first level cascade of centrifuges, maybe a thousand of them running all the time, and you might obtain 10 or 15% enrichment levels. Then you need even better centrifuges to reach the next level. That is what the Natanz facility was supposed to do, which was to reach the next level above 20%, perhaps reaching weapons grade. Destroying the Natanz centrifuge facility has dealt a profoundly serious blow to the Iranian program. I am not sure they have any fissile material right now.

Rod Bryant: How many years do you think that this damage could have set back Iran’s nuclear weapons development?

Stephen Bryen: Anywhere between two and five years if I were to guess.

Rod Bryant: That is buying a little time. A while back, we were speculating that Iran was perhaps a year away from being able to produce a nuclear weapon.

Stephen Bryen: No one says you cannot destroy the next one. I think that is the game everyone is playing. How can we delay nuclear development until perhaps this regime will collapse? Then maybe a new government will arise that may be less dangerous than the current one.

Rod Bryant: That is a brilliant idea. Better than all out total war, for sure.

Stephen Bryen: That is why you do not want attribution. I think that Israel has been incredibly careful for the most part, except when they stole all those documents from the Iranians. Mostly they have been careful to have what we called plausible deniability. I am not worried about that. It is their problem not ours.

Rod Bryant: If Israel were involved in this, there had to be an amazing amount of inside coordination from sympathizers inside Iran would not you think?

Stephen Bryen: That is an interesting question, because if you use inside people, you take a risk of leaks. Big risk of leaks. There is no sign in this deal that any inside people were involved. There were a couple of arrests, but they were let go because they had nothing to do with it. I think bottom line is you would not use inside people. You would use highly trained commandos that you would insert into the places with the right equipment. Then you would use what we call a kinetic cyber-attack to create the havoc that we have witnessed. By that time, the commando teams are long gone. That is the real trick.

Rod Bryant: What you are saying is the cyber-attack was possibly cover for exfiltration to get out of the country.

Stephen Bryen: No. I am saying that these were sleepers. Because they had commando teams put the explosive devices in place so they could be activated remotely. Then when the D-Day came, somebody just launched the cyber part of the attack to set off the explosions.

Rod Bryant: Interesting.

Stephen Bryen: I think that is the most logical way to do it. However, I am not a covert operations analyst. Whoever did it

was brilliant.

Jerry Gordon: Stephen, you mentioned earlier that the missile base and production center was attacked, and you thought that Iran may have had the capability of fitting a nuclear warhead?

Stephen Bryen: I do not think I quite said that I said they were working on it. That was my judgement. I have no proof one way or the other. First, the attack seemed precise. It was not the whole place; it is a huge complex. The assault went after one node that was of high interest. Someone knew that in one node there was a target. If you go after a singular node and not the whole thing or no other parts, it would have been more productive from an explosion point of view. Then you will have a surgical operation going after a specific target. That is what it looked like to me. The only target I would think worth the time and trouble would have been something nuclear.

Jerry Gordon: Having said that, what has been the history of cooperation between North Korea and Iran on this matter?

Stephen Bryen: We know they are cooperating. We know that the North Koreans have shared a lot of technology. But by the way, we do not know that the North Koreans have a delivery system either. We are certain they have nuclear devices. Nuclear design starts with something large. If you took the US program back in World War II, The Manhattan Project, the first bombs were like 4,000 to 5,000 pounds. Huge. You cannot put those on a missile. We could not even easily put them on an airplane. We finally figured out a way to get them into a B-29. They had a pit under the runway where the bomb was, and they had a hydraulic jack just to lift the bomb into the aircraft. A lot of work went into that.

Rod Bryant: We have seen how military technology has evolved to miniaturize nuclear warheads. We also realized that if we can do that it would not be long that even with a full embargo on Iran, that they would have full-blown capabilities of

missile technology to deliver nuclear weapons. We have been discussing these cyber assault and explosions in Iran, and how it might have involved Israel. I had asked Jerry to discuss the Stuxnet codes and what telltale signs that Israel was possibly involved in the development of this code?

Jerry Gordon: That was a lead in Stephen Bryen's article in *The Asia Times*. He said, "This may have been son of Stuxnet." What we want to clarify is what was the Stuxnet project back in 2010 and peculiar aspects of the code in the malworm virus that were related to Queen Esther, and a major Persian Jewish leader who was hanged by the Iranian regime in May of 1979.

Steve Bryen: Let us talk about what Stuxnet was. It was an alleged joint project involving the US and Israel in 2010 to come up with a way of damaging Iran's nuclear program. The objective was to take out Iran's centrifuges through a cyber-attack. The challenge was that Iran's centrifuges were not in any way connected to the internet. Somehow, the virus or mal worm had to be imported into the facility. Someone unknowingly was used to carry it in, and it spread through Bluetooth. That should tell you about how safe your computers are. Stuxnet impacted both the industrial controller, which was Siemens's PC7, STEP 7 industrial controller SCADA system. It also hit the programmable control system, which was another set of software and hardware, that came from Finland, but was manufactured in Iran. Both were manufactured under license in Tehran. Stuxnet was designed to spin these centrifuges out of control, so they would break down, and it was successful. Some say about 25% of the centrifuges at the time were damaged beyond repair. The thing that is different now, compared to then, when there was no explosion, there was no fire, there was no attempt to cause destruction, beyond irretrievably damaging the centrifuges. That was Stuxnet. What I call Son of Stuxnet, is different, because it is connected to some form of fire and explosion. Whether that is a bomb we do not know but my guess is, it is. How the bomb got put in there, I do not

know. Somebody took it in. How would they do that? It was a very sophisticated operation. You asked about the code in the original Stuxnet. There was a lot of exploitation of the Stuxnet malworm by western companies who were trying to figure out how this thing worked.

First, it was an encrypted software, so it was extremely hard to even penetrate it. Two things that popped up in the code was, the use of the term Myrtus in English, which refers to Myrtle. That is the Hebrew word for is Hadassah, and Hadassah is Queen Esther. So that was one kind of giveaway, somebody was having fun in Israel on that one. And the second, was a number, 19790509, one single number, which was supposedly a number to stop the process from continuing. It referred to May 9th, 1979, which was the date on which Habib Elghanian, an Iranian or Persian Jew, was executed in Tehran, because he was objecting to the regime. When that happened, the Jews started leaving. He was a very prominent citizen in the Jewish community. Iran's Jews were afraid, so they left.

Rod Bryant: At some level, he was a gatekeeper for the community, wasn't he?

Stephen Bryant: Yes, absolutely. So, it was a tragedy, but I think that the homage to him in Stuxnet was on purpose.

Rod Bryant: I think that was brilliant. I want to talk about the new Israeli intelligence satellite, Ofek-16. What do we know about it? What are its capabilities?

Stephen Bryen: Well, it is a follow up to the existing ones that they have. However, it has more refined cameras and multiple sensors. The Israelis are looking for any signs of test explosions. I think that is the number one thing, and then, of course, they are looking for any movement in the nuclear program, any shipment of equipment, changes in status, anything they can pick up. They are doing 24/7 monitoring.

Rod Bryant: What types of sophisticated sensors are we

talking about?

Stephen Bryen: Radiation sensors, heat sensors, vibration sensors, all kinds of sensors. There is a chance the Iranians may explode the warhead underground. Now seismically, you might be able to pick it up, but if it is small, you may see some disturbance on the ground.

Rod Bryant: I just assumed that when you exploded something underground, it would not take long for radiation to seep out of the ground

Stephen Bryen: It depends where the underground explosion occurs If it is down deep in a salt mine where there is a strong cap, it may not leak radiation right away.

Jerry Gordon: Do these satellites have what I call LIDAR, ground-penetrating radar?

Stephen Bryen: I do not know if Ofek has that. Ground-penetrating radar. It is a good tool, but it has limitations because usually it requires a lot of power to be effective. Some of these LiDAR systems are mounted on vehicles as you cannot really do it from outer space. What you can do from outer space, which we have done it for years, is monitor missile launches. Now that Israel has an Arrow 3 Anti-Ballistic Missile, which can go out of the atmosphere, they are moving towards the ability to attack missiles just after launch, rather than waiting for them to come over your territory.

Rod Bryant: That has been a discussion that we have had about American air defense systems. The most effective one is one that takes out the missile before it even leaves that region.

Stephen Bryen: That is what Brilliant Pebbles was all about in the Reagan era SDI program. We never did it. Now they are talking about it again. I think within a few years, we will have space-based tests.

Rod Bryant: After the Reagan era, was there a program to at least start that system set up in space to have that capability. Do you think we have that capability at all right now?

Stephen Bryen: No. We do not. We have a sensor capability, but we have had that all along. You could say "Oh look, they fired a missile at us. Isn't that terrible." But what are you going to do about it? If it is on course towards us, we are in big trouble.

Rod Bryant: Do we have the ability to take down a satellite?

Steve Bryen: We can take down a satellite, but the satellite's not a nuclear missile. Satellites run on a predictable path. It is visible. There are a lot of things about a satellite that make it an easy target to destroy. When you are shooting at a missile that has multiple warheads, some of which are real, some which may be decoys, which are released into a pattern, that are sometimes erratic, and you have to find the needle in the haystack and do it within a few milliseconds, it's a tough problem. That is why you want to take them down before they release the warheads, if possible, when they are just off the launch pad.

Rod Bryant: In the case of Israel, you want to stop that before Iran develops long range missiles.

Stephen Bryen: Iran already has the missiles to target Israel and Europe.

Rod Bryant: Right. Overall, if you were going to give a grade Israel on their ability to protect the country from nuclear attack from Iran, what grade would you give them?

Steve Bryen: B+.

Rod Bryant: B+. Wow, incredible.

Stephen Bryen: I think I would grade the United States an F

minus. We are in a terrible mess. I am worried about us.

Rod Bryant: We are out of time. Stephen. We really appreciate your input to this show. We look forward to having you come back next time. Until next week, we say shalom.

Listen to this *Israel News Talk Radio – Beyond the Matrix interview* with Dr. Stephen Bryen.

Watch the Netiv-online YouTube video of the interview with Dr. Stephen Bryen.

«**Previous Article Table of Contents Next Article**»

Jerome B Gordon is a Senior Vice President of the *New English Review,* author of *The West Speaks,* NER Press 2012, and co-author of *Genocide in Sudan: Caliphate Threatens Africa and the World,* JAD Publishing, 2017. Mr. Gordon is a former US Army intelligence officer who served during the Viet Nam era. He is producer and co-host of *Israel News Talk Radio–Beyond the Matrix*. He was the co-host and co-producer of weekly *The Lisa Benson Show for National Security* that aired out of KKNT960 in Phoenix Arizona from 2013 to 2016 and co-host and co-producer of the *Middle East Round Table* periodic series on 1330amWEBY, Northwest Florida Talk Radio, Pensacola, Florida from 2007 to 2017.

Rod Reuven Dovid Bryant is creator and host of *Israel News Talk Radio–Beyond the Matrix*.

Follow NER on Twitter @NERIconoclast