TAG-Org

Talal Abu-Ghazaleh Organization

C4ISR Summit Middle East (Kuwait)
24th to 25th Sept. 2018

C4ISR - Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

Talal Abu-Ghazaleh
Sept. 24, 2018

How best to equip forces to establish joint cyber-defense operations and build cyber resilience

25th Sept. 2018

Intelligence briefing 9.30am – 10.00 am – one of 3 speakers.

Other speakers include:

- Brig. Gen. Randolph Staudenaraus, Chief, Office of Military Cooperation, US State Department, Kuwait
- Lt Col Arnel David, Chief of Staff for the Army, Future Studies Group, US Armed Forces

Dr. Talal Abu Ghazaleh – Talking Points

- We can learn a lot from our friends in the Western intelligence agencies who for many years have worked closely together on cyber defense; we need to develop a strong alliance for an ever-evolving state-of-the-art regional research and training center brand of cooperation in this region and, indeed, move to a new level focused not just on defense, but also on cyber resilience.
- I use the term "cyber resilience" deliberately, over "cyber security" or "cyber defense." Security has a connotation of "locking down," and "keeping the 'bad guys' out." But we must recognize that all networks are likely to have been penetrated and that the challenge is to absorb damage and keep fighting, emerging stronger after the stresses and shocks. This is what I mean by resilience. Defense is important but it alone is not sufficient. In any case, cyber defense needs to include both passive and active components.
- Joint approaches to cyber threats are now key in the face of the extent of the cyber challenge. It is clear this is an urgent, global issue; the keyword here being 'Global'. We cannot afford to live in silos in the face of such belligerence, be it for terrorism, extortion, theft, deception, disruption, or political objectives. A common threat needs a coordinated approach; the basis of which is rapid information analysis and intelligence sharing.
- Developing joint, comprehensive cyber strategy programs must be on the top of the agenda and be an integrated part of our overall military strategies in the region.
- I think it serves us well if we can identify the problem. In cyber warfare, we are protecting national IT assets – hardware and software – wherever they may be, from being exploited. This can happen through:
    1. Sophisticated programs that exploit vulnerabilities in IT assets
    2. Government users that are: duped into installing malicious programs; click malicious email links or fooled into giving up credentials.
    3. Introducing foreign hardware that load viruses onto computers.
    4. Being overwhelmed by denial of service attacks.

       These can be addressed by our countries developing joint cyber strategies that cover people, processes and technology (PPT) to effectively protect our Critical Network Infrastructures (CNI) as well as getting major backbone ISP's to jointly work with them to block amplified attacks against our networks.
- Cybersecurity alone is not enough. Concepts such as cyber resilience and mission assurance are critical We need to act not react to the threats and attacks our military staffs to be able to identify, and respond to these attacks; we need to encourage a mindset throughout our military to protect our information systems; this requires processes to provide pragmatic governance and legislation and the latest cyber security tools and technologies to mitigate such threats.

- We need to adopt a proactive stance and develop early threat warning systems. No single country in our region can nor should do this in isolation. We have to build intelligence command and control centers in our countries that work together, that pool and analyze intelligence for the common good. We cannot afford to take a passive stance and need technology experts to help us bolster our regional defenses and
- foster greater joint cyber defense cooperation.
- I call for greater work to be done to establish a regional cyber command center that can police our regions' electronic border at its very edge. A well-staffed, well-funded regional security operation center (SOC) will provide a strong line of first defense and form the basis for resilience. Once such threats reach our countries, it is already too late. We much stop such attacks before they reach us and develop effective offensive as well as defensive measures. Our previous attempts at cooperation have been well intentioned, but all too fragmented.
- I do not see why we cannot develop an integrated cyber security strategy for all of our countries. Do we really need to reinvent the wheel in each of our countries? Local implementation of this cyber strategy will certainly vary -- depending on budgets and resources -- but a core element is the protection of our Critical Network Infrastructures (CNI).
- Our Ministries of ICT's (MOICTs) in the region must take a leading role in such a vital defense mechanisms in order to push local implementations and develop a resilient and deterrent cyber security capacity, supported by relevant cyber laws, regulations and procedures. They must work much more closely with other ministries and local intelligence agencies to put down practical frameworks for such cooperation; establish effective Computer Emergency Response Teams (CERTs) and ensure we have adequate National Crisis Management Centers in place that can anticipate and act swiftly and decisively to a cyber security breach.
- If our governments do have the required expertise to build such a cyber ecosystem, let us employ the expertise of our friends in other parts of the world. Ignorance is no longer a valid excuse.
- We must also start to develop our own regional cyber security research and development innovation centers. This will help to develop the needed professionals to strengthen our cyber resilience capabilities and also provide a valuable source of income as cyber resilience-related companies take root. We can fulfil the need for cyber resilience specialists and technologies globally. Cyber resilience must become a major export for this region.
- The newly developed University I have established called TAGUCI, excels in producing innovators. I was instrumental in ensuring that one of its specializations is Cyber Security and I look forward to extending this to cyber resilience. No student will graduate unless they produce a unique innovation. We need to build cyber resilience innovators in this region and contribute to the protection of national defenses globally.

Talal Abu-Ghazaleh