How Cyber Warfare and Information Operations are changing Everything!

Presented by
Dr Leigh Armistead, CISSP

Wednesday 16 March 2022
10:00 - 16:30
State University of New York at Albany , USA

This one-day seminar presents an overview of the key issues which are of concern in today's challenging world of cyber warfare and cyber security.

There is increasing concern that our systems are vulnerable to attack from numerous sources and that these attacks are becoming more and more sophisticated. It is therefore essential to understand these threats and to be able to create and implement a robust policy of self defence.

This programme takes participants through all the important issues to be considered to ensure that cyber attacks do not disrupt an organization's operations.

Program outline

1000 What is Information and Cyber Warfare?
- Why are they different than the traditional focus on Air, Land and Sea capabilities?
- Theoretical IW versus Reality.
- How have the elements of power changed over the last two decades?
- At the Strategic Level, who controls this power?
- If it is not the USG, how can we influence it?
- How did we protect the US previously, and can we do that now?

1115 Break

1130 Is there an Operational element of IW?
- If so, who owns it, what is there span of control and influence?
- B-Roll, Positive stories, the strength of trust via relationships.
- What can we not control?
- Historical Examples: Revolutionary War, Vietnam, Desert Storm, Iraq and Afghanistan
- Disinformation Campaigns by foreign/domestic groups
- People's inherent bias and belief's

1230 Lunch

1315 Offensive vs Defensive IW
- Does it matter? Who can do it? Are you allowed?
- If so, do you have trained personnel?
- What about blowback at the strategic/operational level?
- From a military aspect, what is in scope?
- Long-term strategic US objectives
- Medium/Short-Term operational missions
- Safety of US sailors/soldiers/airman/marines

1430 Break

1445 Examples of Current IW Ops

- Russia
- China
- North Korea
- Iran

1530 Break

1545 Moving forward – what should we expect?

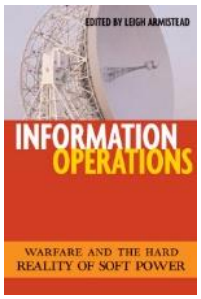
- Ransomware to government / corporations
- Online propaganda to influence diplomatic/military ops
- More attacks from aboard on service members families
- ICS Systems are more vulnerable
- Social Media off-line
- The IoT is an attack vector

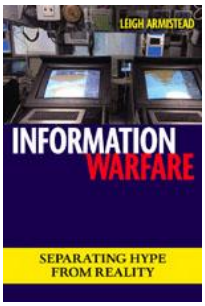
1615 Summary

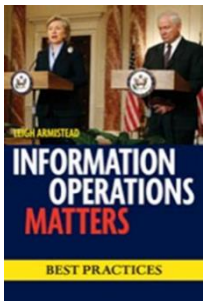
1630 Close of Day

Seminar facilitator

Dr Edwin "Leigh" Armistead is the Principal of ArmisteadTec LLC, a Veteran-Owned Small Business (VOSB) that is certified by the Small Business Administration (SBA) as a Historically Underutilized Business Zone (HBZ), https://www.armisteadtec.com/. This company primarily focuses on the academic functions of Information Warfare (IW), to include curriculum development, teaching as well as other related tasks to include lecturing and writing. A retired United States Naval Officer, Dr Armistead has significant Information Operations academic credentials having written his PhD on the conduct of Cyber Warfare by the federal government and has published three books, in an unclassified format in 2004, 2007 and 2010, all focusing on full Information Warfare. He is also the Chief Editor of the Journal of Information Warfare (JIW) https://www.jinfowar.com/; the Program Director of the International Conference of Cyber Warfare and Security and the Vice-Chair Working Group 9.10, ICT Uses in Peace and War. Shown below are the books on full spectrum cyber warfare and the JIW:







The Seminar will run from **10:00** until **16:30** on Wednesday 16th 0f March 2022 at **State University of New York at Albany , USA**

The attendance fee is **£60**. Fees include an electronic copy of the course materials. To reserve a place please email Elaine Hayne on Elaine@academic-conferences.org