CyberPro

August 25, 2011

Keeping Cyberspace Professionals Informed

THOUGHT LEADER PERSPECTIVE: DR. Panayotis Yannakogeorgos

NSCI's Charles Winstead recently had the opportunity to interview Dr. Panayotis "Pano" Yannakogeorgos, of the Air Force Research Institute (AFRI). Dr. Pano is a Cyber Defense Analyst and Faculty Researcher at the Air Force Research Institute. His research is focused on the impact of malicious cyber activities on global and military affairs, and the establishment of global norms of behavior for cyberspace. He has recently authored chapters titled "Cyberspace: The New Frontier and the Same Old Multilateralism" in Global Norms: American Sponsorship and the Emerging Pattern of World Politics (Palgrave 2010), and "Pitfalls of the Private-Public Partnership Model" in Crime and Terrorism Risk: Studies in Criminology and Criminal Justice (Routledge, 2011). Prior to his current assignment, Dr. Yannakogeorgos taught graduate level courses pertaining to globalization, security and intelligence at Rutgers University's Division of Global Affairs, where he also served as Senior Program Coordinator, and headed the Center for the Study of Emergent Threats in the 21st Century. He has participated in the work of global cyber security bodies including the High Level Experts Group of the Global Cybersecurity Agenda of the International Telecommunications Union. In 2006 he served as an Adviser within the United Nations Security Council on issues related to nuclear non-proliferation, the Middle East (including Iran), Al-Qaida and Internet misuse. Dr. Yannakogeorgos earned his Ph.D. and M.S. in Global Affairs from Rutgers University and an ALB in Philosophy from Harvard University.

NSCI: Can you tell us a little bit about the Air Force Research Institute and their role as it relates to improving cybersecurity?

Pano: The Air Force Research Institute conducts specialized research projects for the Air Staff and DoD to enhance national security and to provide relevant research for the United States Air Force. AFRI also partners with Allied International Military Air Chiefs on research projects. AFRI supplements the Air University and Air Force idea-generating capacity and supports air and space research inquiries from the Chief of Staff, as well as other top-level decision makers throughout DoD, and Defense Industry. Just as digital information and communications technology has revolutionized warfare, and all aspects of life in the developed world, so is AFRI charged with revolutionizing our service through conducting independent research, outreach, and engagement to enhance national security and assure the effectiveness of United States Air Force within the cyber domain.

NSCI: What are AFRI's cyber-related research priorities over the next year or so? Is AFRI interested in collaboration with industry and other academic institutions on these?

Pano: Broadly, we focused on challenging conventional wisdom on understanding the cyber domain to provide an ubiquitous strategic cyber perspective to inform the creation of new defense operating concepts. In 2012, we will be focused on researching cyber power within the context of a broader study on the Asia-Pacific region. In an effort build robust partnerships with other U.S. government department

and agencies, the private sector and academia to enable a whole-of-government cyber strategy, AFRI is sponsoring a conference titled *Cyber Power: The Quest for a Common Ground* on October 26-27, 2011 at Maxwell AFB in Montgomery, AL. This is part of our effort to contribute to a better understanding of the structural sources of cybersecurity challenges, and to identify a common methodology that will serve as framework for identifying solutions and better informed policies.

NSCI: How does AFRI share their research needs and results with industry and academia? How does someone go about getting more involved with AFRI's efforts?

Pano: Through the three pillars of research, outreach, and engagement, we seek to improve the ability to take full advantage of cyberspace's potential by enhancing the capability of our service by engaging in intellectual discourse, and welcome opportunities for interaction and dialogue with individuals and organizations on subjects relating to cybersecurity. AFRI manages the Air University Press, which publishes books, monographs, and occasional papers that are the results of unique research by AFRI researchers, military authors and civilian scholars. AFRI hosts the DoD's flagship *Air & Space Power Journal* on-line and in print. Additionally, AFRI is home for the Strategic Studies Quarterly (SSQ), an Air Force-sponsored Strategic Forum for Military, Government, and Academic Professionals. In the past year, SSQ has featured a special issue on cyber as well as articles by Gen. Michael Hayden and Gen. Keith Alexander. The goal of SSQ to serve as a conduit to establish a cybersecurity conversation between members of the military, government and the academic community.

NSCI: How does AFRI's work fit with the recently released DoD cyber strategy? Do you have any current efforts you can share with us?

Pano: Prior to their articulation in policy, AFRI's research has been focused on supporting the ideas contained within DoD's five pillars for operating in cyberspace. We are sponsoring a conference on *Cyber Power: The Quest for a Common Ground*. This initiative is new and innovative way to enable smart partnerships with a whole-of-government approach with our interagency partners. We aim to aid in the building robust international partnerships during our Asia Pacific study to inform the development of international shared situational awareness that will enable collective self-defense and collective deterrence for the US and our international partners. Of course, there are certain cyber myths enshrined within elements of the DoD strategy. AFRI is making it a priority area to enhance DOD and USAF cyber policies by providing relevant research.

NSCI: There has been a lot of talk concerning legal and policy implications of various cyber-related courses of action.

A. How do you think we provide more clarity in these areas so our senior leaders can make more informed decisions?

B. What do you see as the key legal and policy gaps associated with deterring and responding to cyber attacks targeting the U.S., to include possibly executing our own cyber attacks?

Pano: On the first question, AFRI aims to refine the conceptualization of the cyber domain, in addition to dispelling certain cyber myths. Currently there is a disconnect between the policy communities and the technical communities. This leads to policies being made that are uninformed by technical realities. At the same time, some technologies misunderstand the strategic and national security implications of their work. There no purpose for cyberspace but to serve human operators, and create effects in the physical world. Focusing on technology rather than the characteristics that wholly compose the cyber environment creates the impression that this domain is not connected with the real world. Through a demystification of each sectors domain, we aim to craft their solutions based on both technical and strategic realities. AFRI aims to serve as a "translator" between these two communities so as to bridge this gap.

By way of answering your second question, one key policy gap associated with deterrence is the cyber myth that attribution is required for deterrence. One project I am working on challenges this view. The common view is that deterrence is made difficult because we don't know who created an effect in cyberspace. The result is a focus on resolving the problem with communications protocols that will enable better identity management. Such suggestions overlook the crux of the attribution challenge. Cyber attacks crossing national jurisdictional boundaries exploit poor international cooperation resulting from a lack of harmonized cyber security action plans at the national level to implement technological, managerial, organizational, legal and human competencies into national security strategies to enhance cooperation. This is a root cause of the cyber attribution challenge. I argue that nation-states must be held responsible for bringing to justice any individual, group or entity committing any malicious acts within their cyberspace. Voluntary norms of behavior developed within United Nations over the past decade could guide a doctrine of state responsibility. I am proposing a policy framework to guide US sponsorship of these norms to catalyze the establishment of a robust system of monitoring, controls and sanctions to ensure that the Internet functions as a trusted and heavily defended environment.

You will be able to read all about it in an AFRI monograph titled: Resolving the *Cyber Attribution Challenge: A Global Policy Response* due out from AU Press in December 2011. Prior to then, I am available to speak on this issue to any community that wishes to discuss the details.

NSCI: Cyber situational awareness seems to be an area we really need to improve upon. There are obviously a lot of pieces to that puzzle - sensors, data, analysis, assessment, visualization, and others. How do we get our arms around it and at least get started in providing the needed capabilities? What do you see as a few of the most challenging issues in this area?

Pano: The main challenge is getting past the cultures of secrecy that exist both within government and the private sector and inhibit the sharing of data that will provide a shared awareness and understanding of vulnerabilities and threats within the cyber environment. Currently, the lack of data sharing is a roadblock on the way towards a unified national effort to secure cyberspace, and inhibits the full understanding of threats and vulnerabilities. Mobile technologies and the distributed cloud environment present new challenges to this old problem. We aim to identify what data needs are, and what challenges exist to sharing threat and vulnerability data, and offer insight on how to create

common data structures to allow for rapid information sharing essential to enhancing security in the continuum from mobile to the global cloud.

Two panels at AFRI's *Cyber Power: The Quest Towards a Common Ground* will focus on resolving some of these issues by bring joint and interagency partners along with private sector stakeholders to discuss data needs and structures as well as common analytics and visualization.

NSCI: There seems to be some ongoing debate regarding the reality and urgency of cyber threats. What do you think is needed to convince the naysayers?

Pano: Since 1988, the Morris Worm demonstrated vulnerabilities and attack vectors to a broader constituency, the reality and urgency of cyber threats has been spoken to. For two decades, naysayers have been downplaying the threats and vulnerabilities. With the increasing and very public attacks on military, government, corporate and individual's digital infrastructures; naysayers today are being relegated to gadfly status. Indeed, many proponents of the idea that there is a reality and urgency to cyber threats were naysayers only five, three, one years ago. The more challenging debate today is not how to convince the naysayers that vulnerabilities exist which can be exploited to cause notorious effects, but how to balance privacy with security when discussing appropriate cybersecurity measures. Unfortunately, the naysayers have dominated the debate for the past two decades, and the discussions we are having today should have been addressed at least a decade ago.

NSCI: Is there anything else you'd like to add?

Pano: Thank you for your time, and we look forward to welcoming many of your readers to AFRI's conference on *Cyber Power: The Quest Towards a Common Ground* on October 26-27, 2011 at Maxwell AFB in Montgomery AL (http://afri.au.af.mil/cyber/)

NSCI: Thank you very much for taking the time to visit with us.