Reflections on
Elizabethtown College Ware Seminar on Cyber Security
292 people attended

Tuesday, 9/17/13, 7:00pm-9:00pm, Elizabethtown College Student Center Event Space (KAV)
Videotaped for possible later distribution (C-span, etc) once release received from all panelists and their affiliated institutions/companies

SCHEDULE EXECUTED

6:00pm: Dinner and review of aversion of this document

7:00pm: Susan Traverso PhD (Etown Provost) Introduction to College, Event, Sponsors, Seminar Organizers

Joseph Wunderlich PhD (Etown Assoc. Prof. of Engineering):

Brief intro listing speaker names & titles, and that **101 questions** were solicited from students and faculty, then reviewed by speakers to incorporate into 15-minute talks and Panel Discussion

SCOTT BORG, DIRECTOR & CHIEF ECONOMIST, U.S. CYBER CONSEQUENCES UNIT (CCU)
(Independent nonprofit research institute frequently consulted by top government officials, major Universities, and media throughout the world)

- Scott lectured for 1-1/2 hours to my Engineering and Computer Science students yesterday, we then spent the day together until midnight touring the college, dinner, etc.
- He is unquestionably one of the world's leading authorities on cybersecurity policy and methods, and the worlds leading authority on the economic impacts of cyber attacks

(Talk: How vulnerable is U.S. economy & infrastructure to cyberattack) – primarily questions# 1, 67, and 81
(During panel, open to all 101 questions – selected questions directed exclusively to him)

JOHN SMITH, SENIOR COUNSEL, RAYTHEON CO.
(Company with 68,000 employees and $25B in annual revenue)

- Raytheon's first cybersecurity lawyer and first chief privacy lawyer
- Previously Served similar role in President George W. Bush's Whitehouse
- Clerked for Supreme Court Justice Samuel Alito when Judge Alito was on the US court of appeals
- Magna cum laude from Princeton and Brigham Young University Law School
- Missionary for The Church of Jesus Christ of Latter-day Saints
- Fluent Russian and Ukrainian

(Talk addressing legal-related cybersecurity issues at Rayteon)
(Requested panel questions [exclusive]: #4,9,11,13,14,15,18,32.1,39,42,43,44,45,47,59,60,63-modifed)

IAN WALLACE, BROOKINGS INSTITUTION VISITING FELLOW FOR CYBER SECURITY
(Security and Intelligence Foreign Policy Center)
(Public policy organization in DC conducting research that
(1) Strengthens American democracy;
(2) Fosters economic and social welfare, security, and opportunity; and
(3) Secures a more open, safe, prosperous, and cooperative international system.)

- Extensive cybersecurity policy research including military issues, and private vs. public roles
- Previously Senior official for British Ministry of Defense for 17 years
  - Developed UK's cyberstrategy and cyberrelationship with the US
    - Most recently at British embassy in DC as Defense Policy Councilor and Nuclear Councilor
    - Harvard fellow at Weatherhead Center for International Affairs including researching military implications of new cyber capabilities.

(Talk addressing UK and US cybersecurity policy including military implications)
(During panel, open to first 87 questions below – selected questions will be directed exclusively to him)

PANEL WITH PRESELECTED QUESTIONS (from 101 questions below)

- ***No audience questions***
- ***Questions will be asked specifically of each panelist***
- ***Please don't ask specific questions of other panelists***

PANEL QUESTIONS for SCOTT BORG (depending on degree questions answered during his talk)

(Emphasizing economics, infrastructure, policy, and detailed methods)

A. 88.Can you please tell us (more on) how your team has yet to find an impenetrable system throughout the world (ASKED)

B. 89.Can you please tell us (more on) how distributed sustainability can help with cybersecurity (ASKED)

C. 90. Can you please tell us (more) about the day by day progress of a breakdown in civilization after a cyberattack

D. 91.Can you please tell us (more) about how air traffic control is disabled during cyberattack

E. 92.Can you please tell us (more on) how game theory is used for cybersecurity

F. 93.Can you please tell us (more on) how modularizing systems can help with cybesecurity (ASKED)

G. 94.Can you please tell us (more on) how electrical power load-balancing can help with cybesecurity

H. 95.Can you please tell us (more on) how some simple password-entering timing methods can stop many cyberattacks

I. 96.Can you please restate the five key steps of a cyberattack and elaborate on which step(s) is now the most critical

J. 97.Can you please tell us (more about) the openness of various US administrations and agencies over the past decades to your input

K. 98. Can you please tell us (more on) the details of Edward Snowden (ASKED)

L. 99.Can you please tell us (more on) how you cybersecurity information spreads at various conferences around the world

M. 100.Can you please tell us (more on) the details of the increasing vulnerability of industrial control systems (ASKED)

N. 101.Can you please tell us (more on) cloud computing and cybersecurity

(EXTRA QUESTIONS)

73. How is cybersecurity threatened if everybody embraces communications that use strong encryption to hide the content of their messages, as well as TOR to hide the parties sending and receiving? *TOR is free software for enabling online anonymity. It directs Internet traffic through a free, worldwide volunteer network of more than three thousand relays to conceal a user's location*

76.China is frequently accused of not honoring intellectual property rights. What are the areas of overlap between these concerns and cyber security?

86.How long could a place like the LA basin sustain without water if a cyber attack damaged the infrastructure for obtaining water from the main canal?

84.To what degree can crisis be avoided by US and coalition development of strategically-engineered software to disarm weapons from afar?

83.What are the long-term economic impacts to the US, EU, and other developed nations if Russia and China were to strengthen their technology exchange.

35,61. Is Moore's law going to make brute force password attacks trivially easy in the near future, and do you foresee stronger cryptographic algorithms to compensate for stronger computing power?

4.With the rise of potential cyber threats, would it be appropriate to take a step back and not use advanced technology to monitor basic resources such as our power-grid and water-supply?

38.Do you think cryptocurrencies like Bitcoin will ever have a chance of taking over a substantial portion of the economy?

82.To what degree could Stock exchanges be disrupted by direct electronic tampering, or by panic due to real or perceived cyber-attack?

10. Does your organization create strategies for corporations to prevent cyber attacks?

25. How did the USCCU come up with the cyber security checklist and why do you think it is important to have it available in other languages?

PANEL QUESTIONS for JOHN SMITH

(Emphasizing legal and private-sector issues)

A. 43,14.Is there a way to increase security while maintaining the public's privacy, and what role does anonymity play in cybersecurity? (ASKED)

B. 11,47. How does your previous work as primary legal advisor to the White House Homeland Security Council compare to your present work at Raytheon, and what where the first issues you faced as Raytheon's first cyber security lawyer? (ASKED)

C. 63,15. What is the state of cybersecurity law given that most laws were written before computers played such a significant role, and what kind of legislation is required to address current cyber-security problems? (ASKED)

D. 60. How difficult is it to partake in cybersecurity programs, while maintaining privacy, due to a lack of precedence in Supreme Court rulings?

E. 42.What kind of precautions can an individual take to increase their own cyber security?

F. 13.Other than creating more secure programs, what measures should be taken to address cyber security threats?

G. 9.What drew you to the field of cyber security?

(ASKED): Please give us the analogies that you had planned to include in your talk, but ran out of time

(EXTRA QUESTIONS)

59.Do you think securing the county's cyber and physical infrastructures is a top priority for national security?
18.How important is cyber-security to the private sector?
32. Do you believe our biggest threats to cybersecurity are domestic or international?
39.Are you annoyed by inaccurate portrayals of cyber attacks and hacking in the media & Hollywood?

PANEL QUESTIONS for IAN WALLACE

(Emphasizing international policy and military issues)

A. 87,78. How do political philosophies, cultural histories, and religious views influence governments and peoples to either help, or look the other way, when terrorism threatens -- and what percentage of the world views US efforts to maintain world peace as a positive thing? (ASKED)

B. 4.With the rise of potential cyber threats, would it be appropriate to take a step back and not use advanced technology to monitor basic resources such as our power-grid and water-supply? (ASKED)

C. 73.bWhat should be the proper US response to allegations of computer hacking by the Chinese Military?

D. 75.Some Chinese research universities have been named by the US government as irresponsible in selling computer information to rogue states. How serious are these allegations?

E. 33,55.Does substandard cyber security in other countries indirectly put relatively well-secured countries at risk of attack? How so?

F. 79.To what degree is the United Nations useful in preventing cyberterrorism, and can we rely on the UN to support US security efforts? What are the risks of acting unilaterally? (ASKED)

G. 80.To what degree does the cold war continue, and what role does Russia play in cyberterrorism or cybersecurity.

(EXTRA QUESTIONS)

69. With advancing technology and the fact that there will never be an achievable end to the battle of cyber-security, would you advise that the upcoming generations try not to be so dependent on the internet to lessen damage of a potential attack?

85.To what extent can EMP technology, and HAARP-type systems help with national defense (ASKED)

12.From your experience developing the UK's cyber-relationship with the US, do you believe that most developed nations could sustain a cyber-attack and retaliate with ease? *– and could this prevent nations from fighting – i.e., detante*

49.How do the UK and US policies compare?

Un-edited questions from EGR/CS332 and EGR/CS434 students, plus one high-tech professor:

1. What is the most damage a cyber attack could do to the economy?
2. John M. Smith: What was the most interesting case you had defended in terms of cyber security?
3. Ian Wallace: Have you felt threatened with how quickly technology exploded in terms with your peace keeping amongst nations?
4. In today's world, with the rise of cyber attacks threats, would it be appropriate to take a step back and not use such advanced cyber technology to monitor our basic resources/needs such as electricity supply, water supply, etc. ?
5. With the problems and fears that the Cloud creates, wouldn't it be more wise for people to stick to hardware that they would physically own ?
6. Is it possible, today, to pass through all the security checks done all over the internet and on other networks ? In other words, is it possible to not be watched by the government and still keep our way of communicating with the world ?
7. What are the most immediate threats to cyber security currently in the U.S.?
8. Is a perfectly invulnerable cyber security system possible? If not, what are the limitations?
9. What drew you (any speaker) to the field of cyber security?
10. For Scott Borg. While your organization investigates the consequences of cyber attacks, does your organization generate strategies and proactive measures for corporations to prevent these cyber attacks? If yes, how?
11. For John Smith. How does your previous job working as the primary legal advisor to the White House Homeland Security Council staff compare to the private corporation, Raytheon Company, you currently work at?
12. For Ian Wallace. From your previous work experience developing the UK's cyber relationship with the United States, do you believe that most governments and large corporations could sustain a cyber attack and retaliate with ease?
13. Other than creating more secure programs, what measures should be taken to address cyber security threats?
14. What role do you believe anonymity plays in cyber security? How would you address the problems it introduces?
15. What kind of legislation if any is required to address our current problems with cyber security?
16. What parameters are used to determine if something should be considered a threat?
17. What have you learned in your time as director of the U.S. Cyber Consequences Unit?
18. How important do you think cyber-security is to the private sector?
19. What was the most advanced virus that ever found/intervened? That you have found/intervened?
20. What exactly could a cyber attack mean for us as a nation?
21. How prepared are we to offset a cyber attack?
22. Their opinions on the current state of the NSA
23. Compare the "cyber preparedness" of China and the United States
24. How secure is my personal computer?
25. Scott borg – How did the USCCU come up with the cyber security checklist and why do you think it is important to have it available in other languages?
26. John smith – What is Raytheon's SureView technology and has it found any potentially dangerous threats?
27. Ian Wallace – What experiences have you had working with the department of defense in the UK that led you to your research area?
28. How confident can the U.S. public be that the government won't pass new cyber security laws that conflict with the public interest unknowingly?
29. How prepared overall do you believe the U.S. government is in terms of cyber security?
30. Does your work endanger the private sector's cybersecurity measures that are already in place?
31. Scott Borg: What kind of measures are currently in place to guard against the impact of potential breaches in vital cyber systems?
32. John Smith: Are our biggest threats to cyber security domestic or international? Who should we be looking out for?
33. Ian Wallace: Does substandard cyber security in other countries indirectly put relatively well-secured countries at risk of attack? How so?
34. Do you think two step authentication will become standard for website logins in the near future?
35. Is Moore's law going to make brute force password attacks trivially easy in the near future?
36. What is the best way to defend a server against DDOS attacks?
37. Do you see any threat from networks like TOR which cannot be effectively regulated?
38. Do you think cryptocurrencies like Bitcoin will ever have a chance of taking over a substantial portion of the economy?
39. Are you annoyed by inaccurate portrayals of cyber attacks and hacking in the media & Hollywood?
40. Are you ever contacted by studios that want to do things accurately?
41. How can we make cyber security more secure?
42. What kind of precautions can an individual take to increase their own cyber security?
43. Do you think that there is way to increase security while still maintaining the public's privacy?
44. Why is the cyber security a bigger threat now than it used to be?
45. Why is there so much panic about a potential cyber attack that will cause the public to panic when there has never been an attack like such before?
46. Do you believe that the cyber initiative should be county wide or vary state by state?
47. John Smith - what sort of issues did you face as the first cyber security lawyer at Raytheon?
48. Scott Borg - what are the basic steps that your group takes when you discover a cyber attack?
49. Ian Wallace - how do the UK and US policies compare?
50. Scott Borg: The CCU is independent of the government but still consults with them on numerous cases about cyber security. Why was it decided that the CCU should exist when the government has several departments that do pretty much the same thing?
51. John M. Smith: What is a "crime" relating to cyber security that most people aren't aware of but you do on a daily basis?
52. Ian Wallace: Cyber terrorism is one of the worst threats to our National Security. What countries do we need to worry about when it comes to U.S. cyber security?
53. Scott Borg: What is the main part of the economy that would be affected by a cyber attack? What do we (America) need to prepare for to fight this?
54. John M. Smith: What type of cyber security cases have you currently dealt with?
55. Ian Wallace: What would happen to the U.S. if cyber terrorism occurred in the UK or neighboring country?
56. For all three of them: For the common consumer who goes on the internet daily who log on to their internet accounts, what is the best way to protect themselves from internet hackers? For example, is it best to have a really long password, such as a sentence, or should we have a smaller password with confusing symbols?
57. For all three of them; What is the most difficult cyber security crime to identify or catch? For example phishing scam or fake identities.
58. For all three of them: Should Americans be concerned about the invasion of privacy from the White house? What do you three think they are worried about?
59. Do you think securing the countries cyber and physical infrastructures is a top priority for national security?
60. John Smith: How difficult is it to partake in cyber security programs while maintaining privacy due to a lack of precedence in Supreme Court rulings?
61. Do you foresee stronger cryptographic algorithms in the future to compensate for stronger computing power coming in the near future?
62. Do cyber attacks pose more of a threat than physical attacks?
63. Because laws weren't written with computers in mind, are there still loopholes that allow cyber criminals to go unpunished? *Rewording: What is the state of cybersecurity law given that most laws were written before computers played such a significant role?*
64. If advanced technology has made cyber attacks one of the most serious threats to society, has it also allowed for greater defenses?
65. How do the US and UK policies differ with regards to cyber security policy?
66. How does the government handle cyber security differently than private companies?
67. Scott Borg: Besides a cyber-attack on infrastructure, what other type of attacks do you look for and believe could pose a threat to the economy?
68. John Smith: Is religion reflected in what you look for with-in cyber security? (An example would be appreciated)
69. Ian Wallace: With advancing technology and the fact that there will never be an achievable end to the battle of cyber-security, would you advise that the upcoming generations try not to be so dependent on the internet to lessen damage of a potential attack?

70. "Mr. Borg, how do we all know that we're safe from terrorist attacks? Do you have intelligence on Al-Qaeda every hour?" Is this too much?
71. "Mr. Smith, since religion plays a big role in your job, between law and religion, do you ever have any problems with people who don't take religion serious enough?"
72. "Mr. Wallace, after reading your article on the Daily Beast, i was wondering; Since more and more devices are getting connected to the internet, will that make it more difficult for the Cyber Security to monitor threats?
73. Whether or not the allegations that Edward Snowden made about the actions and capabilities of the NSA are true, we can agree that governments (and some companies such as Google) can read many of our electronic communications. What are the implications for the future of cybersecurity if what is now a relatively unsophisticated general population begins to embrace modes of communication that use strong encryption (such as AES) to hide the content of their messages as well as anonymization (such as Tor) to hide the parties sending and receiving them? Is this change likely to happen?

Questions from D.Kenley PhD :

73.bWhat should be the proper US response to allegations of computer hacking by the Chinese PLA? *(accidently not numbered initially)*

74. What should we expect the Chinese response to be regarding allegations of US cyber spying?
75. Some Chinese research universities have been named by the US government as irresponsible in selling computer information to rogue states. How serious are these allegations?
76. China is frequently accused of not honoring intellectual property rights. What are the areas of overlap between these concerns and cyber security?

Questions from J. Wunderlich PhD:

77. What other countries in the world are committed to helping the U.S. police the world? Or should we not view ourselves this way?
78. What percentage of the world's governments and peoples view US efforts to maintain world peace and promote democracy as positive, and what percentage would rather have us not intervene at all, and/or view us as simply an imperial power protecting our own interests.
79. To what degree is the United Nations useful in preventing cyberterrorism (or any type of terrorism or crimes against humanity). Can we rely on the United Nations to support U.S. security efforts? What are the risks of acting unilaterally?
80. To what degree does the cold war continue, and what role does Russia play in cyberterrorism and/or cybersecurity.
81. What role does China play in cyberterrorism and/or cybersecurity, and to what degree does China need or want the US. Economy to remain stable?
82. To what degree could Stock exchanges be disrupted by cyberterrorism; by both direct electronic tampering, or by panic due to real or perceived cyber-attacks.
83. What are the long-term economic impacts to the US, EU, and other developed nations if Russia and China were to strengthen their technology exchange.
84. To what degree can present or future crisis in rogue nations armed with weapons of mass destruction be avoided by US and coalition development of strategically-engineered software to disarm these weapons from afar?
85. Although this is not a cyber-question, it is a very technical one: To what extent can EMP technology, and HARP-type systems be deployed to disable weapons of mass destruction (i.e., not just long-range missiles)
86. How long could a place like the LA basin sustain without water if a cyber attack where to damage the capability of this region to obtain water from the canal coming from the north.
87. How do various political philosophies, individual histories, and/or religious views influence governments and peoples to either help or look the other way when terrorism threatens.
88. Scott Borg: Can you please tell us (more on) how your team has yet to find an impenetrable system throughout the world
89. Scott Borg: Can you please tell us (more on) how distributed sustainability can help with cybersecurity
90. Scott Borg: Can you please tell us (more) about the day by day progress of a breakdown in civilization after a cyberattack
91. Scott Borg: Can you please tell us (more) about how air traffic control is disabled during cyberattack
92. Scott Borg: Can you please tell us (more on) how game theory is used for cybersecurity
93. Scott Borg: Can you please tell us (more on) how modularizing systems can help with cybesecurity
94. Scott Borg: Can you please tell us (more on) how electrical power load-balancing can help with cybesecurity
95. Scott Borg: Can you please tell us (more on) how some simple password-entering timing methods can stop many cyberattacks
96. Scott Borg: Can you please restate the five key steps of a cyberattack and elaborate on which step(s) is now the most critical
97. Scott Borg: Can you please tell us (more about) the openness of various US administrations and agencies over the past decades to your input
98. Scott Borg: Can you please tell us (more on) the details Edward Snowden
99. Scott Borg: Can you please tell us (more on) how you cybersecurity information spreads at various conferences around the world
100. Scott Borg: Can you please tell us (more on) the details of the increasing vulnerability of industrial control systems
101. Scott Borg: Can you please tell us (more on) cloud computing and cybersecurity

CLOSING REMARKS:

Thanks to President, Provost, Director of Center for Global Understanding and Peacemaking, and financial supporters

Special thanks to Ambassador John B. Craig (for panel and moderator)

PRESENTLY:

- Ambassador-and-Scholar-in-residence at Elizabethtown College since 2002
- Chairman of the Board of the Jadwin Group, a prominent international venture capital company
- At this moment, helping with important government matters oversees

DEGREES:

- B.S. from American University's School of International Service
- Master's in International Relations from the National Defense University
- Honorary Doctorate from Elizabethtown College

PREVIOUSLY:

- Appointed by President Bill Clinton as U.S. Ambassador to Oman
- Appointed by President George W. Bush, immediately after 9/11,
- as Special Assistant to the President, and Senior Director for Combating Terrorism
- Regional Vice President for Boeing Aircraft
- Director of Arabian Peninsula Affairs in the Department of State
- Deputy Chief of Mission in Damascus Syria, and Bogota Colombia.
- Speaks French, Arabic, and Spanish.