50 CYBER QUESTIONS

Every Airman Can Answer

Dr. Kamal T. Jabbour, ST
Senior Scientist
Information Assurance

Preface and Acknowledgements

This compilation of answers to 50 selected cyber questions addresses the scientific and technical angle of flying, fighting and winning in cyberspace. We did not intend this book as a glossary of Internet terms, a dictionary of acronyms, or a doctrinal essay on warfare in cyberspace. Wherever possible, we substituted scientific facts for personal opinions, and brought to bear thirty years of engineering practice in computer networks and cyber security.

We wish to acknowledge the contributions to this book of Col Fred Wieners (USAF Retired), Col Bill Gray (USAF Retired), Dr. Kevin Kwiat, Dr. Daniel Pease, Dr. Paul Phister, Paul Yaworsky, Sonja Glumich, Brian Kropa and Jerry Dussault.

Dr. J

Approved for public release by WPAFB Public Affairs.
Disposition Date: 5/7/2008
Document Number: WPAFB 08-3194

This is an AFRL publication. We are working with the AF Doctrine Center to develop an AF approved version.

50 Cyber Questions Every Airman Can Answer

Compiled by

Dr. Kamal T. Jabbour, ST
Senior Scientist
Information Assurance

1. What is the Mission of the US Air Force?

The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in Air, Space, and Cyberspace.

2. What is Cyberspace?

Author William Gibson coined the term cyberspace by combining *cybernetics* and *space* into the term cyberspace in his 1982 story "Burning Chrome" and popularized it is his 1984 novel Neuromancer. Gibson described cyberspace as "*a consensual hallucination experienced daily by billions... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data*."

In the minds of many, cyberspace became synonymous to the Internet. In September 2006, the Joint Chiefs of Staff endorsed a definition of cyberspace as "*a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures*."

We dissect this definition to derive the scientific basis of its intent. The word "domain" instead of "environment" carries legal implications under the laws of armed conflict. "Electronics and the electromagnetic spectrum" refer to the wave-particle duality of radiation which, when modulated with information, creates a signal. "Data and networked systems" refer to digital information and application programs, and the computers and networks on which they exist, in other words data and applications, at rest and in motion.

For warfare purposes, we derive a working definition of cyberspace as “a domain in which signals hold at risk intelligent systems.” This definition recognizes three components to cyberspace: (1) the “effectors” encompass a broad range of signal-borne threats, analog and digital; (2) the “medium” enables effectors to access the targets, wired and wireless, hardware and software; and (3) the “targets” include weapons and systems that use computers or networks.

This working definition of cyberspace effectors is consistent with Department of Defense Information Operations (IO) Security Classification Guide that excludes from consideration as IO weapons those conventional weapons that produce IO effects.

3. What are the Differences among Data, Information and Intelligence?

Data refer to low-level digital signals that tend to be time-sensitive but disorganized. Information derives from organizing data in a logical manner. Intelligence refers to information placed in a contextual framework.

4. How does Cyberspace Differ from Traditional War Fighting Domains?

Fundamental differences between cyberspace and the traditional war-fighting domains of land, sea, air and space include:

- low cost of entry: anyone with a computer and an Internet connection can launch attacks against global US interests;
- anonymity through unauthenticated protocols and anonymizers; and
- jurisdictional uncertainty by transcending international borders.

The above challenges create legal implications on the authorities governing cyber defense, including from United States Code (USC) Title 10 for military activities, Title 18 for criminal activities, Title 32 for National Guard and state defense, and Title 50 for foreign intelligence surveillance.

5. Why are Cyberspace Effects Important to Mission Success?

The increased reliance on Information Systems to accomplish mission critical tasks gives cyberspace effects an increasing influence on mission success. If a task or process requires information that can only be conveyed electronically, that task or process is potentially vulnerable to cyberspace effects. Additionally, if a platform or system interacts electronically with information, the operation of that platform or system depends potentially on the integrity of that information. There are a myriad of ways even subtle cyberspace effects can influence mission operations due to this class of dependencies.

6. Why does the Air Force Require a Separate Cyber Command?

Cyberspace is increasingly critical and inseparable from our national power and interests. Adversary denial of the domain to US military operations can take away battlespace awareness, command and control, and precision strike, and leave our exquisite 21st Century capabilities paralyzed. We cannot afford to let this happen so now is the time to focus on a consolidated effort to protect and defend the domain.

In 2003, the White House published "The National Strategy to Secure Cyberspace," a document that presented cyberspace security as a subset of Homeland Security and outlined a wide range of initiatives to "protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States."

One of those initiatives calls for the government to "improve coordination for responding to cyber attacks within the U.S. national security community." The Air Force answered that call in December 2005 when it added cyberspace to its mission statement.

7. What are Information Operations?

Information operations (IO) refer to the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC) - the Five IO Core Capabilities - in

concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

Capabilities supporting IO include information assurance (IA), physical security, physical attack, counterintelligence (CI), and combat camera. These are either directly or indirectly involved in the information environment and contribute to effective IO.

Related IO Capabilities consist of public affairs (PA), civil-military operations (CMO), and defense support to public diplomacy.

8. What is the Information Environment?

The Information Environment consists of three conceptual dimensions: physical, information and cognitive:

The physical dimension is the tangible real world. It represents the devices, systems, computers and networks that constitute weapon systems. The physical dimension includes also the stored computer programs and applications that impart utility to this dimension.

The information dimension is where information is created, manipulated, shared, and stored. This dimension links the real world of the physical dimension with the human consciousness of the cognitive dimension.

The cognitive dimension is where the individual processes the received information against norms, beliefs and values. The cognitive dimension evaluates and processes information via an Observe-Orient-Decide-Act (OODA) loop, and communicates decisions to the physical layer.

9. What is Information Power?

Information power refers to the ability to use information resources and forces to create discernable military and political effects. Together with airpower and space power, information power can help put friendly forces in a position of advantage. Information power is an inseparable part of the air and space power concept. Information power can be applied through kinetic (heat, blast, and fragmentation—bombs and bullets, basically) or nonkinetic means (through weapons or techniques that persuade, confuse, surprise, or contribute to the security of our forces). Further, information power can create lethal or nonlethal effects.

For Airmen, our information power capabilities contribute directly to the joint force campaign in several ways. First, these capabilities help prepare and shape the overall information environment for the joint force commander before, during, and after combat. Second, information power capabilities provide situational awareness to Air Force commanders about to employ air and space forces to achieve the objectives of the joint force commander. Third, information power can create real physical or psychological effects upon our adversaries. These effects may be discrete (individual) effects. More often however, information effects enhance or support other physical or psychological effects created by other air and space forces. Finally, information power capabilities can support other air power or space power missions.

10. What is a Revolution in Military Affairs?

A Revolution in Military Affairs (RMA) refers to a theory about future warfare linked to concepts, organization and technological changes. In the context of cyber warfare, RMA refers to the dichotomy of military superiority enabled by net-centricity, and the commensurate vulnerability of kinetic weapon dependency on cyberspace.

Famous RMAs in history include the English longbow that gave Henry V victory over the French army in the battle of Agincourt in 1415, and the rifled musket that decimated the Confederate Army in Gettysburg in 1863. The success of the strategic bombardment RMA in World War II depended on a technology-enabled industry-driven superiority. In contrast, the success of cyber warfare as an RMA depends on an education-enabled technology-driven framework.

11. What is Information Assurance?

Joint Publication 3-13 defines Information Assurance (IA) as a set of measures that protect and defend information and information systems by ensuring their confidentiality, integrity, availability, authentication and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IA is a Supporting Capability for Information Operations. IO depend on IA to protect information and information systems, thereby assuring continuous capability. IA and IO have an operational relationship in which IO are concerned with the coordination of military activities

in the information environment, while IA protects the electronic and automated portions of the information environment. IO rely on IA to protect infrastructure to ensure its availability to position information for influence purposes and for the delivery of information to the adversary. IA relies on IO to provide operational protection with coordinated OPSEC, EP, CND, and CI against adversary IO or intelligence efforts directed against friendly electronic information or information systems.

12. What is Confidentiality?

Confidentiality seeks to ensure that secrets remain secret. It deals with protecting data and programs from unauthorized access and display. Internet privacy concerns revolve around accidental and intentional disclosure of personal information, and therefore a failure of confidentiality. Strong encryption suffices often to protect data and programs from unauthorized access, but encryption alone does not protect against malicious or negligent insider threat.

13. What is Encryption?

Encryption refers to an arithmetic operation that uses a key to transform a message from plain text into ciphertext. Cryptography is the study of encryption techniques, while cryptanalysis refers to the study of methods to break encryptions.

Private key cryptography uses symmetrical encryption, where the encryption key is the same as the decryption key. The Data Encryption Standard (DES) is an example of private key cryptography. Public-key cryptography uses asymmetric encryption, with different encryption and decryption keys. The RSA algorithm is commonly-used in public-key cryptography.

14. What is Integrity?

Integrity refers to the protection of data and programs against unauthorized modification. Data bases of enemy targets, airmen medical records, supplies purchase orders and rendezvous coordinates for tankers and fighters are susceptible to data modification with potentially catastrophic consequences. Cyber attack vectors have targeted recently computer applications and operating systems with a more advanced threat to system integrity.

15. What is Availability?

System availability and data availability refer to at will access to resources. As traditional war-fighting domains depend increasingly on cyber assets, the uninterrupted availability of hardware and software assets plays a vital role in mission accomplishment. Denial-of-service attacks undermine the availability of cyber assets.

16. What is a Distributed Denial of Service Attack?

Distributed Denial of Service (DDoS) attacks flood a network resource, like a Web server, with huge amounts of data from many different machines and locations in an effort to bring the server down and deny its availability. DDoS attacks deny users access to the information and services residing on the resource. The attacks can be launched from information systems across the Internet unified in their efforts, or by compromised information systems controlled by servers that hide the true origin of the attack.

17. What is Authentication?

Authentication refers to identifying digitally, and with certainty, the identity and need-to-know of an access request to a cyber resource. Digital signatures, trusted certificates, two-form factors and biometrics provide various means of authentication with differing strengths. Although authentication verifies with high probabilistic certainty the identity of a user or process accessing a resource, authentication alone does not provide for attribution.

18. What are Attribution and Non-Repudiation?

Attribution refers to tracing back the origins of an authorized or an unauthorized access to a resource. Non-repudiation refers to holding accountable a verified and authenticated access to a resource. Attribution and non-repudiation are interchangeable for authorized accesses. Since the Internet operates on inherently unauthenticated protocols, attribution and non-repudiation collide often with anonymity. Obfuscation techniques, source address spoofing and anonymizers increase the difficulty of attribution.

19. What Role does Attribution Play in Deterrence?

Classic deterrence relies on threatening a potential adversary with an overwhelming use of force as a means to dissuade unfavorable action. In the cyber framework, attribution becomes an essential pre-requisite to deterrence. Motivation and intent play a key role in classical deterrence.

Assured mutual destruction provided nuclear deterrence during the cold war of yesteryear. Assured mutual co-existence provides some form of deterrence in the space domain of today.

Strategic deterrence considers return on investment (ROI) as the principal metric in dissuading hostile activity. Deterrence in a culture where the ultimate sacrifice is a normal part of life, and where attribution becomes inconsequential, necessitates reducing significantly the potential rewards. As investment approaches infinity, deterrence works best by reducing potential return to zero. Thus, strategic deterrence in cyberspace seeks to minimize or neutralize the potential gain from an attack as a means to deterring it.

20. What are Network Warfare Operations?

Network Warfare Operations (NW Ops), a subset of cyber warfare operations, are the integration of the military capabilities of network attack (NetA), network defense (NetD), and network warfare support (NetS). The integrated planning and employment of network warfare operations along with electronic warfare operations (EW Ops), influence operations, and other military capabilities are conducted to achieve desired effects across the information domain. Network warfare operations, when employed with other information operations, ensure our ability to operate in a contested information environment.

Network Attack (NetA) employs network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks.

Network Defense (NetD) employs network-based capabilities to defend friendly information resident in, or transiting through, networks against adversary efforts to destroy, disrupt, corrupt or usurp it.

Network Warfare Support (NetS) is the collection and production of network related data for immediate decisions involving NW Ops. NetS is critical to NetA and NetD actions to find, fix, track and assess both

adversaries and friendly sources of access, as well as vulnerability for the purpose of immediate defense, threat prediction and recognition, targeting, access and technique development, planning and execution in NW Ops.

21. What is the International Standards Organization (ISO) Open System Interconnection (OSI) Reference Model?

The ISO OSI Reference Model consists of seven layers, and seeks to standardize interfaces among network software and hardware manufacturers. The primary function of the Physical Layer is to provide an ordered bit pipe. The Data Link Layer provides a virtually error-free link by breaking the data stream into packets, and implementing error detection and retransmission. The Network Layer allows routing among nodes and networks. The Transport Layer provides host-to-host transport that shields the underlying network infrastructure. The Session Layer enables session management through login and logout, authentication and passwords. The Presentation Layer deals with data presentation, data compression and encryption. The Application Layer interfaces the user to the network through special-purpose and general-purpose applications.

The IEEE 802 and the Internet Protocol (IP) standards map loosely onto the ISO OSI Reference Model. The PHY Layer maps to the Physical Layer. The MAC (Medium Access Control) Layer maps to the lower half, and the LLC (Logical Link Control) maps to the upper half of the Data Link Layer. IP maps onto the Network Layer. TCP (Transmission Control Protocol) maps onto the Transport Layer, and protocols like HTTP (HyperText Transfer Protocol) belong to the Application Layer.

22. How fast do Electrons Travel in Cyberspace?

Contrary to general belief, electrons do not travel at the speed of light, even in cyberspace. Quantum theory defines the speed of light as the speed at which a photon travels in free space, at about 300 million meters per second. Weighing 9.11 x 10-28 gram each, electrons are too heavy to accelerate to the speed of light. Since electrons are charged particles, their motion generates a fast propagating electromagnetic field that can reach speeds of 200 million meters per second on an electrical cable, about two-thirds the speed of light in free space.

23. What is Cyber Warfare?

Cyber warfare refers to the use of information and signals to deliver effects against military systems. The access media in cyberspace include all forms of data storage and transmission, physical and virtual, static and dynamic, electronic and optical. Network warfare is a subset of cyber warfare that uses networks – particularly the Internet – as the access medium.

Cyber warfare integrates the three capabilities of cyber offense, cyber defense, and cyber warfare support.

24. What are the Technical Challenges in Cyber Offense?

Cyber Offense deals with delivering precision effects against a range of adversary targets to affect his perceptions and will to fight. The fundamental cyber offense challenges facing the S&T community consist of access, stealth and effects.

25. What does Access to Adversary Systems Entail?

Access refers to the challenge of delivering and installing an intelligent agent on a target system. The agent may consist of hardware or software, and provides a command, control and communication architecture. Target systems of interest to cyber warriors include a wide range of intelligent systems from desktop computers to personal communication devices (cell phones), embedded command and control systems (flight avionics) and Supervisory Control and Data Acquisition (SCADA) systems.

Exercising an attack vector against system vulnerability provides a common technique for delivering an effect onto a target. Vulnerabilities occur at all network protocol layers. Attacks against the Physical Layer may take the form of physical modification of a system; attacks against the Network Layer may exploit Internet Protocol vulnerabilities through malformed packets or stack overflow; attacks against the Session Layer may employ social engineering to obtain a user password; and attacks against the Application Layer may use email to target an individual.

The ability to access remotely a vulnerable computer system connected to the Internet becomes harder with common information assurance practices, and difficulty escalates for closed systems isolated from the Internet. Proprietary systems pose additional access challenges, as do active avoidance and deception procedures.

26. What is Stealth and Persistence in Cyberspace?

Successful access to a target system and the installation of an intelligent agent carry little value unless the agent can persist and survive normal operations. To a malicious agent, the host system presents a potentially hostile environment fraught with virus scanners, intrusion detectors, malware sanitizers, systems re-installation and hardware upgrades. The survival of the agent and its persistence as a command and control platform for payload delivery depend on its ability to hide, morph and masquerade.

Agent developers play a cat-and-mouse game with malware detectors, in what shapes up as a long-drawn out battle. On the surface, this battle favors the offense given the proliferation of hiding places in a computer. However, secure virtualization techniques and an engineered introduction of custom hardware for securing trust promise to level the playing field and increase the stakes.

27. What does it mean to Deliver Precision Effects?

Delivering cyber effects refers to the D-family of “deter, deny, disrupt, deceive, dissuade, degrade, destroy and defeat” adversary systems through lethal and non-lethal means. The impact of these effects ranges from user annoyance, through system control, all the way to affecting the will of a nation to follow a desired course of action.

Delivering precision effects became synonymous to low-collateral damage in some doctrinal circles. This narrow interpretation ignores meaningful historical lessons where high-collateral damage constituted a desired precision effect. The Doolittle raid on Tokyo on 18 April 1942 delivered the precision effect of shaking the confidence of the Japanese military in their ability to protect the Emperor, and the bombing of Hiroshima and Nagasaki delivered the precision effect of an unconditional Japanese surrender.

Understanding the full range of possible D-effects permits cyber warriors to develop technologies and tactics to operate across a broad range of targets. In addition to providing the National Command Authority (NCA) with true sovereign options in cyberspace, an unconstrained approach to cyber offense S & T carries immediate dividends to cyber defense. By divorcing intent from technology when modeling the cyber threat, and by recognizing the reality that some adversaries may not play by our rules, a defender expands his toolkit to provide much broader utility against irregular threats.

28. What are Cyber Threats?

The traditional method to examine threats is to classify them according to the motivation and intent of the actors:

- Hackers and crackers – seek notoriety
- Criminals – seek financial benefit
- Terrorists – seek ideological gain
- Nation states – seek political and military advantage

A technology look at threat focuses on risk and vulnerabilities, regardless of motivation and intent. The National Institute of Standards defines the risk to information systems as a function of the likelihood of a given threat exercising a particular potential vulnerability. As the complexity of computer and network systems increased, the potential vulnerabilities increased correspondingly. Risk mitigation must therefore seek reductions in both threat and vulnerability.

29. What is DRFM?

Digital Radio Frequency Memory (DRFM) is a high-speed digital storage device that can operate at radio frequencies. Equipped with proper antennas, an analog-to-digital converter on the front end

and a digital-to-analog converter on the back-end, DRFM can store and replay very high frequency signals in the Gigahertz range. This capability permits DRFM devices to mount replay attacks against a range of cyber systems, mimicking the exact properties of the original signal without the need to break its encryption.

30. What is Phishing?

Phishing refers to an application layer threat in which attackers combine technical deception with social engineering to steal personal information from Internet users. Phishing uses emails with spoofed sender addresses or contents to drive recipients to counterfeit web sites that solicit private information or install malware on the target computer.

Spear-phishing uses more advanced social engineering to target a spoofed email to a specific individual, using detailed knowledge on the victim to customize the subject and content of the email.

Phishing remains a common technique to lure individuals into cyber traps.

31. What is the Difference between a Virus and a Worm?

Both viruses and worms exploit vulnerabilities in the computer network stack to install and propagate malicious code. Viruses require typically user action to infect a machine and propagate to its next target. In contrast, worms propagate automatically from vulnerable machine to vulnerable machine without user action.

For example, the Melissa virus propagated when a user opened an infected attachment in an email. This caused the virus to email the infected document to the alias list found on the victim computers. On the other hand, the Morris Internet worm propagated on its own among Unix computers without user assistance, exploiting any one of several possible operating system vulnerabilities.

32. What are the Tenets of Cyber Defense?

Cyber defense seeks to anticipate and avoid threats, detect and defeat threats, survive and recover from attacks. In an analogy to the OODA loop, cyber defense seeks to operate inside the OODA loop of the threat.

Cyber warfare affords the planners an alternative approach to risk assessment through assumptions. In a game changing thought process, analogous to a shift away from stochastic poker playing towards deterministic chess analysis, the cyber defender possesses the luxury of considering the entire space of threat scenarios, at least a couple of moves deep, and instituting defenses against the most devastating threats, not simply the most likely ones.

33. How does Cyber Defense Anticipate and Avoid Threats?

Anticipating threats and avoiding them eliminates the need to fight them, and saves the concurrent cost to data and system integrity, making prevention an effective first line of defense against cyber threats.

Anticipating a cyber threat includes setting-up over-the-horizon early warning systems that detect anomalous activity, analyze rapidly its forensic fingerprint to predict future behavior, and communicate through reach back viable options to avoid the threat.

From a war fighting perspective, the Internet favored traditionally the defense over the offense. This inherent advantage to the attacker resulted from the design of the Internet Protocols for tolerance to failure rather than resilience to attack. Modifying the cyber domain to favor the defense may provide an effective method for attack avoidance.

Cyberspace domain modification can occur at any of the seven layers of the OSI Reference Model. Just as a carrier battle group sails the oceans rather than sitting still in one location, so can a network or system move around the IP address space for deception and attack avoidance. Polymorphic networks, thin clients and secure virtualization offer potential risk reduction through lower vulnerability.

The tenets of anti tamper protection technologies seek to reduce vulnerability by reducing the scope of protection and focusing on

critical components, the “crown jewels” in a system, and making them harder to access. This approach allows the defenders to impose high penalties on the attacker and deter the threat.

34. What is a Firewall?

A firewall provides network perimeter defense in the form of a network-layer device that enforces on all packet traffic the rules in an Access Control List. A firewall typically allows or blocks packets based on protocol and port, permitting usually unrestricted outbound traffic, but blocking unsolicited incoming traffic. In a layered defense posture, a firewall prevents external devices from connecting to machines inside the firewall perimeter.

35. What is Public Key Infrastructure?

Public Key Infrastructure (PKI) enables users of an unsecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair obtained and shared through a trusted authority. The public key infrastructure provides a digital certificate that can identify an individual or an organization, and directory services that can store and revoke certificates.

The “key” element of the PKI refers to an asymmetric key pair comprised of a Public Key and a Private Key generated simultaneously using an irreversible mathematical process.

The private key is given only to the key owner, and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is not shared or sent across the Internet. The key owner uses the private key to decrypt text encrypted with his public key by someone else.

PKI enables assurances not previously available:

- Confidentiality: prevents unauthorized access to data.
- Integrity: alerts of unauthorized modification of data.
- Authentication: verifies user identity.
- Non-Repudiation: provides attribution.

36. What is a CAC?

The Common Access Card (CAC) is a United States Department of Defense (DoD) smartcard issued as standard identification for active duty military personnel, reserve personnel, civilian employees, and eligible contractor personnel.

The CAC is used as a general identification card as well as for authentication to enable access to DoD computers, networks and certain DoD facilities. It also serves as an identification card under the Geneva Convention. The CAC enables encrypting and signing email, facilitates the use of PKI authentication tools, and establishes an authoritative process for the use of identity credentials.

PKI credentials or certificates are encrypted in the integrated circuit chip located on the front of the Common Access Card (CAC) and protected by a Personal Identification Number (PIN).

37. How does Cyber Defense Detect and Defeat Threats?

Cyber threat detection follows often one of two methods: (1) classifying normal system behavior and looking for anomalies, or (2) looking for a match in a pre-compiled catalog of known malicious activity. The first method suffers from high heuristic complexity and uncertain results, while the second method misses new malware for which no signature exists.

System malfunction and software bugs complicate further threat detection. The ability to discriminate between accidental and malicious activity often requires advanced analysis that eludes automated systems. Insider threat, whether malicious or inadvertent, complicates further threat detection.

Threat defeat seeks to cancel out the adverse effects of threats. Defeat techniques aim to restore the threatened system to a prior known steady state. This restoration may include killing unauthorized processes, uninstalling malicious programs, deleting malicious files and reconfiguring peripherals. However, some result in file deletion, program modification and loss of settings, requiring extensive system recovery beyond basic threat defeat.

38. How do Systems Survive and Recover from Attacks?

The ability to fight through an attack and recover to fight another day characterizes a resilient system. In response to the threat from internal fires and those of (external) torpedoes, naval vessels feature double hulls that permit a ship to survive a direct hit and continue to fight through the battle. Similarly, cyber systems must continue to function properly, albeit at a graceful degradation in the face of an attack.

At the system of systems level, hardware and software diversity increases the ability of a complex system to survive a discriminating attack against a specific class of systems. A zero-day exploit targeting an un-patched vulnerability inflicts more damage on a vulnerable homogeneous system than it does against a diverse heterogeneous system with a mix of machines.

A layered defense in depth makes allowance for successful attacks, and sets in place procedures for post-threat recovery. Cyber attacks result rarely in permanent destruction of systems that necessitate hardware replacement. In either case, recovery necessitates pre-established systematic procedures to restore a system to a known stable state.

39. What is Cybercraft?

Cybercraft provides the root of trust for an integrated cyber defense. Cybercraft resides on friendly computers and weapon systems to provide persistent situational awareness on its environment; collaborates with other cybercraft to map the environment into a layered picture for a command-level view of cyberspace; establishes a trusted command, control and communication architecture; provides a guarantee of self-protection that drives a formal description of its state, and thereby implements the intent of the commander by deploying payloads to defeat threats.

40. What is Trust?

In his speech to the C4ISR Integration Conference, Crystal City, Va., Nov. 2, 2006, Secretary of the Air Force Michael Wynne asked:

"*What new Habits of Thought do we need in order to create and develop technology, and to fight in the 21st Century?"*

The answer is to go back to my comment at the start, and think in terms of Trust. Our operations in each of our Services all rely on Trust.

- *That is, the pilot can trust information that a target is the foe, not innocent inhabitants of a school building or hospital or embassy.*
- *The groundfighter with a communication device can trust that the device is not being tracked by a foe, potentially exposing the ground force unnecessarily.*

This New Way of War is data-dependent. So we need to think in terms of Trust and securing Trust."

We consider trust the single most important parameter in cyberspace. From a mathematical perspective, we do not measure trust in binary fashion – one or zero, true or false, present or absent – but rather on a continuum from little trust to a lot more trust.

To a cyber defender, the trust in a defensive posture, such as Cybercraft, provides a measure of the cost to the adversary of defeating this defense.

41. What Technologies Support Cyber Warfare?

Effective cyber offense and cyber defense require support function to visualize the domain, analyze quickly events of interest, and derive timely situational awareness and actionable intelligence.

42. What is Cyber Intelligence?

The newest addition to the "INT" family, CYBINT refers to an automatic process of enumerating a cyber neighborhood, identifying assets, detecting vulnerabilities and developing attack vectors. Cyber intelligence seeks to transform raw network connectivity data into actionable information. In a changing topology due to attack or preventive polymorphism, cyber intelligence plays an equally important role in characterizing the blue assets of the defender as the red assets of an attacker.

Cyber intelligence goes beyond the Intelligence Preparation of the Battlespace (IPB). The former takes into consideration both players in a cyber conflict, while IPB tends to focus on the target of an attack. In this context, cyber intelligence refers to the use of intelligence in support of cyber.

Conversely, cyber exploitation can provide valuable intelligence information on adversary systems. System intrusion may yield valuable information to complete the intelligence picture of an unknown system. In this context, cyber intelligence refers to the use of cyber in support of intelligence.

43. How can Rapid Cyber Forensics Enable Deterrence?

Cyber operations occur in the compressed time domain of milliseconds and seconds, the time it takes for packets to travel among network nodes and for programs to execute on computers. This pace of activity necessitates the automation of defensive steps of threat detection, classification, course-of-action (COA) selection and defeat. These four steps correspond to the OODA loop of Observe a threat, Orient, Decide and Act.

The compressed time scale of cyber attacks necessitates automating the response OODA-loop. In particular, the Orient step necessitates rapid real-time forensics of the blue systems under attack for the purposes of attribution and COA selection. Attribution serves a dual role of identifying the authority applicable to the threat (criminal versus military) and enabling deterrence through active defense. Cyber geo-location, the virtual GPS of the cyber world, increases attribution fidelity by locating the origin of a threat in cyberspace as well as geographically.

Accurate attribution may result in deterrence through the threat of precise retaliation. Deterrence works especially when the motivation for cyber attacks seeks modest Return-On-Investment (ROI). While a common criminal may seek a high return on a small investment, an activist may offer the ultimate investment to achieve ideological returns. Since attribution provides no deterrence to high-investment attackers, trivializing the potential return may produce the desired deterrence.

44. What brings Situational Awareness to Cyberspace?

Unlike traditional domains characterized by geography and time, cyberspace transcends physical boundaries onto logical and virtual dimensions. The layered representation of links and nodes, domains and processes, applications and organizations, complicates further the

development of a Common Operating Picture (COP) of mission impact and capabilities.

Situational awareness (SA) deals with complementary perspectives of cyberspace. At the micro level, SA provides a representation of the environment from the perspective of a node or an agent, where availability and reliability play important roles. At the macro level, SA provides the commander with a high-level view of cyberspace with mission functionality and capability. The mapping of Mission-Essential Functions (MEF) onto the underlying physical infrastructure, and taking into account the fluidity of the intermediate protocol layers, poses a fundamental challenge to cyber SA.

45. What is Steganography?

Steganography is the art and science of hiding data. Unlike cryptography that transforms plaintext into ciphertext, steganography hides data by embedding them into carrier files or vessels. Most common vessels include pictures, audio files and video files, however, any computer file can hide data within its structure.

Steganography uses mathematical techniques to maximize the hiding capacity of a vessel. Steganalysis, the science of detecting and recovering hidden data, relies heavily on signal processing techniques. Oftentimes, cryptographic techniques encrypt the data prior to hiding to mask their properties and make detection even harder.

46. What is Digital Watermarking?

Digital watermarking uses strong steganography techniques to embed uniquely identifiable information inside data files. As its name implies, watermarking seeks to protect the integrity of a file, permits the detection of tampering, and allows tracking and attribution.

47. What is the Difference between Cyber Career Force and Cyber Career Field?

A cyber career force refers to airmen with diverse skills and backgrounds who receive specialized training on commercial network management tools. A cyber career field refers to airmen educated in the science and technology of cyber warfare, covering the gamut of fundamentals from mathematics to physics, linear algebra

to electromagnetism, computer software to computer hardware, electronics to cryptography.

48. What is Cyber Training?

A myth, just like javelin-catching at track meets.

49. What is the ACE?

The Advanced Course in Engineering (ACE) Cyber Security Boot Camp is an elite program to educate the next generation of Air Force officers to command the cyber RMA. Created in 2003 in response to President George W. Bush's National Strategy to Secure Cyberspace, the ACE accepts college seniors in computer engineering, electrical engineering and computer science with a minimum GPA of 3.0 into a ten-week intense residential summer program of graduate education, problem solving, research internships, officer development, weekly 8-mile runs, 24x7 cyber warfare and an all-out capstone winner-takes-all Hackfest.

ACE graduates commission into cyber warfare positions throughout the Air Force, and form the core of officers in the cyber career field.

50. What question did we forget?

Please let us know so we can start compiling the next book of "50 More Cyber Questions Every Airman Can Answer."

Dr. Kamal T. Jabbour, a member of the scientific and professional cadre of senior executives, is Senior Scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, Rome, NY. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. He conceives, plans, and advocates major research and development activities, monitors and guides the quality of scientific and technical resources, and provides expert technical consultation to other Air Force organizations, Department of Defense and government agencies, universities and industry.

Contact Information

Office of the Senior Scientist for Information Assurance
Air Force Research Laboratory, Information Directorate
525 Brooks Road, Rome, New York 13441

Phone 315-330-4370 DSN 587-4370

Email iast@rl.af.mil