

# C4ISR via Dark Webs

## An Alternative Concept for Protecting Critical Information in Contested Cyberspace Environments

Capt Kyle L. Bingman, USAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

The world is increasingly connected, both physically and metaphorically, by the relentless spread of networks such as the Internet and the multitude of devices reaching out for the information it contains. Even further, individuals, organizations, and nation-states are becoming more reliant on this interconnected world for activities from the mundane to the critical. This trend towards greater connectivity is likely to continue on an upward spiral. According to research done by Cisco Systems, global Internet protocol traffic in the past five years has increased fivefold and will pass the zettabyte threshold (approximately 1 trillion gigabytes or  $10^{24}$  bytes) by the end of 2016.<sup>1</sup> At the same time as this astounding development and its consequent benefits for society are occurring, however, cybersecurity incidents have increased. In 2015 over \$75 billion (US) were spent on cybersecurity in an attempt to safeguard protected information from a range of malicious actors including criminals and those working for nation-states.<sup>2</sup> The United States made this outlay despite acknowledgment that the most often pursued method of cyber defense—defense in depth—has failed time and again.<sup>3</sup>

This complex and insecure reality affects not only the civilian world but also the military; the US Air Force is most certainly not exempt from this situation. Instead, with its dependency on integrated communications and weapons systems to carry out key missions, it is the service perhaps most reliant on this incredibly vulnerable construct of networks and devices. Over the years, the Air Force has attempted to posture itself in a manner that allows it to maintain surety and the integrity of its networks and information by using the same defense-in-depth method of cybersecurity as the commercial sector. However, as evidenced by successful attacks against many of the most critical networks, this approach is becoming a losing battle against skilled adversaries who can outpace the development of new defenses.<sup>4</sup> Faced with near-peer cyber actors such as China and Russia, among others, as well as highly skilled independent and transnational actors, the Air Force must find a way to ensure the accessibility and usability of its key information by a means that departs from the status quo. Otherwise, it must accept significant risk during future operations due to adversarial actions taken in cyberspace. This article details the nature of this complex, problematic reality and offers a solution for the service to regain control and the integrity of its key information.

## The Situation

Capabilities designed to connect nodes quickly and share information act as a force multiplier because of gains in effectiveness. The interconnected environment allows military forces to resupply, coordinate, reposition, and share intelligence at incredible speeds. Yet, as much as these capabilities open possibilities for the Air Force, they also expose vulnerabilities. Actors around the globe—from the nation-state level to hacktivists, from China and Russia to Anonymous—recognize this fact as well. Cyberspace is now the first war-fighting domain and, perhaps more specifically, the first and primary target as the default means to initiate hostilities. Leaders in China's People's Liberation Army, for instance, have embraced the idea that successful war fighting is predicated on exerting control over the adversary's information and associated infrastructure. Assessments state that during a conflict, the army would target logistics; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); and other mission-critical systems to delay US force flow into a theater and to degrade war-fighting capabilities.<sup>5</sup> In other instances, individual, unaffiliated hackers have expressed interest in military systems or have conducted attacks that highlighted significant vulnerabilities in military-related networks. These include hacks of satellites and associated systems, attacks that caused physical damage by means of malicious code, and distributed-denial-of-service strikes that significantly degraded globally scaled networks.<sup>6</sup> The examples are innumerable, but a theme runs through them all: the Air Force relies on information systems to manage and operate a high-technology force, but those same systems are at the center of many potential adversaries' targeting bull's-eyes.

Many assessments acknowledge the likelihood that cyber attacks will be successful in degrading military capability and reducing capacity. In the Defense Science Board's 2013 report on the resiliency of military systems in the face of advanced cyber threats, experts noted that "the United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities."<sup>7</sup> The report goes on to say that, among other effects, "weapons and weapon systems may fail to operate as intended."<sup>8</sup> Other assessments are similarly dire in their pronouncements. Alan Shaffer, former assistant secretary of defense for research and engineering, admitted that "the Department of Defense is being challenged for technological superiority in ways we have not seen for many years," including cyberspace.<sup>9</sup> He added that "systems whose capabilities can be negated by cyber-attack offer no advantage to the United States."<sup>10</sup> In subsequent testimony to Congress, Mr. Shaffer went on to say that "this has led to a situation where . . . US superiority in many warfare domains will be at risk."<sup>11</sup> That is, future conflicts are not likely to be ones of *Blue versus Red* as we typically conceptualize conflict but ones of *Blue versus the operational constraints imposed by a contested cyberspace environment as created by Red*.<sup>12</sup> This construct benefits any actor with the desire to create an asymmetric advantage to prevent the United States from performing to its greatest abilities. If America has to fight to present, supply, and coordinate its forces, then the likelihood of success is small as

long as its forces struggle against the constraints rather than expend resources against the adversary. To overcome this situation, US forces must find a way to act *beyond* the constraints in order to conduct C4ISR effectively. Current methods, however, fail to enable this requirement.

## Defense in Depth

At the moment, the method utilized to handle this situation and secure the Air Force's critical systems is the traditional defense-in-depth means of cybersecurity. Developed in the early days of the Internet when security was not a significant concern, defense in depth applied the principles of separation and distance so effective for securing assets in the physical world to the growing cyber world. It did so despite the fact that these physical laws are irrelevant in the cyber domain unless one is referring to the physical infrastructure upon which it exists. With defense in depth, networks are protected by using layers of detection and protection mechanisms such as firewalls, intrusion-detection systems, antivirus software, physical security, and an informed user base. Like an army besieging a castle, defense in depth notionally forces an attacker to expend a large number of resources attempting to find a way into a target network. However, regardless of the significant amount of money and effort put into building these protective mechanisms, they have largely proved ineffective against the most creative and skilled attackers. Instead of attackers being deterred by resource costs required to sustain a siege, the situation reversed itself so that network defenders expend massive numbers of resources in an attempt to withstand almost constant intrusions by the adversary.

Statistics of recent years reveal this unfortunate truth quite plainly. In 2014 the number of reported cybersecurity incidents around the world rose 48 percent; furthermore, another cybersecurity firm reported that as many as 71 percent of compromises go undetected.<sup>13</sup> Additionally, when compromises are detected, approximately 90 percent were enabled by malware targeted and specifically crafted for a particular system, thereby ensuring that it would elude detection or mitigation by commonly used defense-in-depth mechanisms.<sup>14</sup> With over 1 million malware threats released per day, it is no wonder that the cybersecurity firm SANS perceptibly referred to defense in depth as "unsustainable"; indeed, advanced threats are outpacing defenses.<sup>15</sup> Around the same time, the National Science Foundation's Special Cyber Operations Research and Engineering Committee pointedly stated that "defense-in-depth failed to provide information assurance against all but the most elementary threats, in the process putting at risk mission essential functions."<sup>16</sup> The group then went on to speculate whether defense in depth was actually a means to "defer harm rather than a means to security."<sup>17</sup> Such speculation has proved accurate; the defense-in-depth status quo will not protect key systems and information used by the Air Force to carry out operations from the most advanced attackers. Unfortunately, this truth remains largely unacknowledged because of a cultural unwillingness to shift to a new mode of conceptualizing the cyber world.

Continuing to utilize defense in depth as the sole mechanism for cybersecurity adheres to a view of the world in which kinetic conflict was the sole method of war.

This perspective still offers viable solutions for the kinetic world; however, it became less relevant when cyberspace made distance and topography no longer the defining concerns for a military's defense. Attempting to rely only on defense in depth for cybersecurity essentially amounts to trying to protect a three-dimensional world from adversaries with access to a fourth dimension—there is always a way for them to gain access when they can see from a different viewpoint. As Gen Stanley McChrystal, USA, retired, mentioned in a recent talk, defense in depth is effectively a “Maginot Line” method of cybersecurity.<sup>18</sup> It is successful in keeping many less capable or less innovative adversaries out of networks—an assured benefit—but it will also result in the skilled opposition finding a new and less expected way past the barrier. The standard defense-in-depth responses of increasing the layered defense around networks—and even newer initiatives such as using hunter teams as point-defense-type mechanisms—are not going to be completely effective when adversaries have had years to prepare access to networks under defenders' watchful eyes. Change is clearly needed. Any method of defense that is to be truly effective in protecting key information and systems needed for C4ISR must also embrace the characteristics of cyberspace as it truly exists rather than try to make it conform to an outdated understanding that it surpasses and encompasses.

## A Solution

Although the current outlook is bleak, the situation can be improved if Air Force leadership decides to radically alter its current methods of carrying out C4ISR in a contested environment. The service must be prepared to implement an additional, radically different construct for C4ISR that belies any previous method or network and—in all likelihood—that runs markedly against the current common culture of widespread information sharing and common operating pictures. Only through this type of additional defensive option can the Air Force increase the chances of operational success, thereby mitigating the likely actions of a skilled adversary. The following steps detail the main components of a truly viable C4ISR system for contested environments.

### ***Information Prioritization and Risk Assessment***

Prior to the start of a conflict with an adversary who has sufficient capability to disrupt current C4ISR systems and networks, information must be prioritized in terms of its necessity to create effects as well as the amount of risk that can be accepted within a set of information due to deception. Information that is less necessary or for which an acceptable amount of risk can be anticipated or mitigated without notable difficulty should continue to be passed via primary methods. One should do so not only to limit the scope of the additional method of communication detailed below but also to ensure that no noticeable decrease occurs in traffic that could cue an adversary to this method.

### ***Unassociated Infrastructure***

During a conflict, the Air Force must not rely solely on any previously utilized network or system to pass key information or maintain a common operating picture. Instead, it must switch to systems that have never been used and that have been verified in origin to mitigate a potential supply chain or otherwise previously placed malware. Moreover, the service must utilize a network entirely unassociated with the current means of passing military-related traffic. The speed and covert nature with which this new construct must be set up will limit its size and require that only key participants have access to it. Only information deemed essential will be passed via this network. Information for which misinformation or degradation is an acceptable risk can and should still be passed by current methods and systems. Doing so not only will lower the required scale of the network necessary to pass key information but also will ensure that a significant decline in traffic on current networks will not act as an indicator for the adversary. Development and testing of this alternative network—as well as its other components, discussed below—must take place outside the standard acquisitions process to guarantee its unanticipated use.

### ***Commercial Networks and Dark Webs***

Traffic must pass entirely over commercial networks, ideally transiting through and primarily remaining in dark web, peer-to-peer networks such as the Invisible Internet Project or Freenet.<sup>19</sup> Because the Internet is a distributed network of networks constantly reestablishing connections with each other rather than a single, coordinated system, it can essentially self-heal and remain available even under attack; disruptions in routes are temporary and often quickly subverted. The global nature of the Internet also increases its resiliency since effects to one region can be mitigated by shifting to routes through another. Peer-to-peer networks have proved even stronger with this capability, as seen in their numerous, successful evasions of law enforcement's attempts to take them down.<sup>20</sup> This resiliency could be strengthened by augmenting the diversity of possible connection infrastructure from primarily fiber-optic lines; however, the Internet's current state is still strong. Given the amount of traffic transiting the Internet as well as the inherent anonymity of dark web network users, key data would be secured by the obscurity of hiding in plain sight rather than relying on defense-in-depth mechanisms such as firewalls and intrusion-detection systems around known military networks.

### ***Constantly Shifting Data***

Data must not be stored in the same place for a significant period of time. Using technologies such as cloud hosting and the peer-to-peer construct upon which many dark web networks are built, one must shift any large store of information from location to location frequently. Doing so will help ensure that if an adversary does detect this additional method of C4ISR, he will have a difficult time catching up to the numerous shifts and that, if the actor does locate it, he will have visibility for only a short period of time.

### ***Multiple and Redundant Data Paths***

There must be multiple ways to input data to and retrieve it from this dark-web-based information store. One must be able to abandon ties to information paths traditionally considered “secure” for the most crucial information in view of potential compromise by a skilled opponent. Instead, key data must be input into and retrieved from the dark web data store surreptitiously and in the clear by multiple methods—again utilizing the principle of hiding in plain sight. Any source or location could input data by methods including automated posts from all forms of sensors or even less traditional ones such as using chat platforms or forums. By not being dependent on a single method or source, the Air Force gains not only security through obscurity but also resiliency. Further, given the nature of peer-to-peer dark web networks, loss of one information path would not reveal the central store or result in the compromise of other data paths.

### ***“Honeycomb” Information Sharing***

Information fusion and analysis must happen in nontraditional settings not associated with traditional centers such as those throughout the distributed common ground system (DCGS). Because the latter is an existing system, one must assume that it is compromised. Rather than information flowing in a hierarchical manner to a specific group of analysts, it must move throughout weapons systems, analysts, and planners around the world in a honeycomb manner to make full use of processing capabilities as well as data points. Information sources would “push” small notifications of data points that they can provide while requirements could be “pulled” by sources as needed, thereby limiting the amount of traffic passed through the network and aiding in its hiding in plain sight. Since the DCGS construct already has placed analysts and associated requirements around the world, the personnel are in place; however, they must be moved away from known military facilities to new sites equipped with the required technologies. Any or all sites could carry out analysis, but the construct could change this situation throughout the operation, based on the viability of data paths to particular sites. To make this scenario actionable, one would have to conduct a full study of personnel needs for this “all-source DCGS.”

### ***Replaceable Hardware***

These sites and others tied into this new C4ISR network must not rely either on large-scale critical infrastructure or single methods of connection to the Internet. In light of the nature of possible power outages and the chance for compromise, it is essential that any system be able to stand alone and be easily replaced. Consequently, the Air Force must rely on systems more reflective of the current cyber domain, such as laptops and tablets that can be swapped quickly and easily disposed of. Moreover, the service must utilize multiple access points to the Internet, from traditional fiber connections to more open means such as cell networks or public WiFi hot spots.

## *Defense via Deception*

The Air Force must develop a deception capability to assist in hiding the existence of this additional communication method in the event that it is discovered. By flooding the Internet with realistic but deceptive traffic, one could force an adversary to spend a considerable amount of time working to discern which information was real and which was not.

## Conclusion

In essence, these are the tactics of asymmetric actors such as insurgents. This proposed means of C4ISR clearly breaks with the Air Force's current culture of hierarchical information flow and decision making as well as its belief in defense in depth as the most effective means to secure information. Defense in depth as a means of cybersecurity does safeguard networks against lower-level threats and should not be abandoned, but it is not a viable solution for securing the most critical information during a conflict. The solution, one possible conception of which was detailed above, calls for embracing a broader understanding of security that acknowledges the true strengths of cyberspace. By utilizing dark web capabilities, taking advantage of the geographic relativity of cyberspace, and embracing a honeycomb flow of information, the Air Force can overcome the constraints upon C4ISR that an enemy will attempt to place on the service during a conflict.

Adopting such methods would be unconventional. Nevertheless, failing to do so is to ignore not only the fact that the domains in which the service fights have expanded but also that cyberspace is a drastically different realm. By utilizing only models like defense in depth to secure its information rather than accepting the new environment in a way that also takes advantage of its strengths, the Air Force is not protecting its key information in the best possible way but is making it easier for an adversary to find and access that data. Cyberspace operations have the strong potential to negate the effectiveness of the service's operations if the status quo does not change. It is time for the Air Force to accept the true nature of cyberspace and operate there using capabilities designed for success in that domain. 🌟

## Notes

1. "The Zettabyte Era—Trends and Analysis," Cisco, 2 June 2016, <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html>.
2. "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach \$75.4 Billion in 2015," Gartner, 23 September 2015, <http://www.gartner.com/newsroom/id/3135617>.
3. *Defense in depth* is a broad term and can mean, without error, many different things to different people. This article uses the term only to refer to a layered defensive construct for a network that includes technology-based elements such as firewalls and intrusion-detection and -prevention systems, administrative elements such as password policies and bans on removable media, and physical elements such as securing access to hardware components.

4. Numerous examples of critical networks could be cited here. A sampling of the most important, post-Stuxnet, include Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 3 March 2016, <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>; Dan Goodin, "Active Malware Operation Lets Attackers Sabotage US Energy Industry," *Ars Technica*, 30 June 2014, <http://arstechnica.com/security/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/>; Dan McWhorter, "Mandiant Exposes APT1—One of China's Cyber Espionage Units & Releases 3,000 Indicators," FireEye, 19 February 2013, <https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html>; and Nicole Perlroth, "In Attack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, 23 October 2012, <http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html>.

5. Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (West Falls Church, VA: Northrop Grumman Corporation, 7 March 2012), <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf>; and Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015* (Washington, DC: Office of the Secretary of Defense, 7 April 2015), [http://www.defense.gov/Portals/1/Documents/pubs/2015\\_China\\_Military\\_Power\\_Report.pdf](http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf).

6. Tony Capaccio and Jeff Bliss, "Chinese Military Suspected in Hacker Attacks on U.S. Satellites," Bloomberg Technology, 26 October 2011, <http://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites>; and Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, 8 January 2015, <https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>. The example of distributed-denial-of-service attacks is not clearly related to the Air Force but shows how even a small group of technically skilled actors can produce serious effects against large networks. Often accused of "ruining Christmas" just to anger people and doing little to refute the claim, Lizard Squad is an example of the type of rogue actor that should be considered alongside more organized groups when one thinks of conflict in cyberspace. Abby Ohlheiser, "Xbox Live Is Up, PlayStation's Network Still Recovering after Christmas Day Outage," *Washington Post*, 26 December 2014, <https://www.washingtonpost.com/news/national/wp/2014/12/26/playstation-and-xbox-networks-are-still-recovering-from-a-christmas-day-outage>.

7. Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Department of Defense, Defense Science Board, January 2013), [iii], <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>.

8. *Ibid.*, 28.

9. Senate, *Testimony before the Senate Appropriations Subcommittee on Defense, Witness Statement of HON Frank Kendall, Under Secretary of Defense for Acquisition, Technology & Logistics, Mr. Alan Shaffer, Principal Deputy Assistant Secretary of Defense for Research & Engineering, Dr. Arati Prabhakar, Director, Defense Advanced Research Projects Agency*, 114th Cong., 1st sess., 22 April 2015, 12, <http://www.defenseinnovationmarketplace.mil/resources/042215DoDInnovationResearch-JointTestimony-SAC-D.pdf>.

10. *Ibid.*, 7.

11. House, *Statement Testimony of Mr. Alan R. Shaffer, Principal Deputy, Assistant Secretary of Defense for Research and Engineering, before the United States House of Representatives Committee on Armed Services, Subcommittee on Intelligence, Emerging Threats and Capabilities*, 113th Cong., 2nd sess., 26 March 2014, 9, [http://www.acq.osd.mil/chieftechnologist/publications/docs/FY2015\\_TestimonyASD\(RE\)\\_ShafferA\\_20140326.pdf](http://www.acq.osd.mil/chieftechnologist/publications/docs/FY2015_TestimonyASD(RE)_ShafferA_20140326.pdf).

12. In military settings, "Blue" typically refers to friendly forces while "Red" refers to aggressor forces.

13. "The Global State of Information Security Survey 2015— Managing Cyber Risks in an Inter-connected World," PWC, [http://www.pwccn.com/home/eng/rcs\\_info\\_security\\_2015.html](http://www.pwccn.com/home/eng/rcs_info_security_2015.html).

14. Rajendra Dodhiawala, "Why Protection Alone Won't Work Today," CounterTack, 14 December 2015, <http://www.countertack.com/blog/why-protection-alone-wont-work-today>.

15. Virginia Harrison and Jose Pagliery "Nearly 1 Million New Malware Threats Released Every Day," *CNN*, 14 April 2015, <http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security>; and Prescott E. Small, *Defense in Depth: An Impractical Strategy for a Cyber World* (Bethesda MD: SANS Institute, 14 November 2011), <http://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896>.




16. “Assumption Buster Workshop: Defense-in-Depth Is a Smart Investment for Cyber Security” *Federal Register* 76, no. 8 (12 January 2011), <https://www.gpo.gov/fdsys/pkg/FR-2011-01-12/html/2011-522.htm>.

17. Ibid.

18. “Stanley McChrystal,” video, 4:15, Big Think, 2016, <http://bigthink.com/videos/s-mcchrystal-cybersecurity>.

19. The Internet is not the only means to share data among computers; rather, it is simply the most common as well as the most easily accessed because it is publicly indexed. Therefore, it is referred to as the “visible” or “surface” web. Other networks exist that serve a similar purpose but are neither indexed nor accessible without special software. These networks are often referred to as part of the “dark web” due to their security and anonymity. Many of them utilize a decentralized peer-to-peer framework that, along with encryption, makes it difficult to perform traffic analysis on shared data. Although it would be clear to an “observer” that someone was using a service like the Invisible Internet Project, it would be very difficult to determine what was being done or shared.

20. George Dvorsky, “Could Someone Really Destroy the Whole Internet?,” *io9* (blog), 19 September 2012, <http://io9.gizmodo.com/5944558/could-someone-really-destroy-the-whole-internet>.

	<p><b>Capt Kyle L. Bingman, USAF</b></p> <p>Captain Bingman (MA, American Military University) leads intelligence and war gaming for the Center of Strategy and Technology’s Blue Horizons program. She is responsible for directing intelligence efforts supporting the USAF chief of staff’s most forward-looking strategic study, evaluating the impact of emerging and disruptive technology as well as geostrategic trends on defense capabilities. As an intelligence officer with a unique background in cyberspace, Captain Bingman began her career as a part of Detachment 2, 318th Cyberspace Operations Group, where she worked to integrate offensive and defensive cyberspace operations into exercises such as Red Flag and USAF Weapons School events. She then was the senior analyst for the 57th Information Aggressor Squadron, where she led research efforts to ensure that the squadron’s Red Team cyber operations replicated realistic, threat-based tactics. Prior to her current assignment, Captain Bingman was a senior instructor at Squadron Officer College.</p>
--	--

**Let us know what you think! Leave a comment!**

**Distribution A: Approved for public release; distribution unlimited.**

<http://www.airpower.au.af.mil>