An example of an operation with medium dependence on UAS to execute mission-critical tasks would be a major contingency operations (MCO) scenario against a state-level adversary in which UAS serve in support roles such as ISR and communications nodes. For the purposes of this scenario, the manned-unmanned aircraft mix mirrors the current USAF aircraft force structure, minus the MQ-1/9 family of aircraft. Mission-critical assets such as strike and offensive counter-air (OCA) aircraft are almost exclusively controlled by pilots in the cockpit, as are tankers, transports, and battlefield C2 aircraft. UAS assets can fill a variety of roles in this environment in the areas of communications nodes and SIGINT gathering. Aircraft such as the EQ-4 BACN would act as Tactical Data Link (TDL) translators, exploiting their ability to orbit at high altitudes for extended periods of time while translating TDL languages amongst manned assets and C2.[67] Other UAS platforms, including additional versions of the RQ-4 Global Hawk, would be used to gather electronic intelligence (ELINT) on enemy radar and communication systems from a standoff distance generally outside the range of the enemy's defensive missile systems.

If the enemy's capability, reach, and intent were all assessed to be high, a medium friendly dependence on UAS for mission accomplishment would push the EW/Cyber risk to UAS to 18 – just above the high risk threshold. A reduction in any one aspect of enemy ability to a medium level – for example, to account for an unknown quantity as mentioned in the Definitions section above – reduces the overall risk level to the medium range as shown in Table 3 below.

		Friendly Dependence on UAS	**Total Risk**
Enemy EW/Cyber Capability	3	Medium (x2 Multiplier)	**16**
Enemy EW/Cyber Reach	2		
Enemy EW/Cyber Intent	3		
	1-12: Low Risk	13-17: Medium Risk	>17: High Risk

Table 3. Risk Matrix Results for Medium Dependence

High Friendly Dependence on UAS

A high dependence on UAS systems for mission accomplishment can generate a variety of outcomes, from low to high risk levels for EW/Cyber effects on friendly UAS, depending on their capability.

This current nature of US conflicts in Iraq and Afghanistan involve enemies with very little ability to harm unmanned aircraft using EW/Cyber tools. To reflect this scenario, low scores are assigned to the enemy capability, reach, and intent categories, with a high friendly dependence multiplier indicating the extensive use of unmanned systems by the US. This produces a 9 (low) overall risk level – friendly forces are essentially able to operate unmanned aircraft in any way they see fit, with little danger of enemy interference in the EW/Cyber spectrum.

Should the enemy in those or similar conflicts acquire a medium level of capability and reach with a corresponding medium level of intent to employ it, the risk increases to 18 – just above the high threshold if friendly forces continue with a high dependence level. These results are shown in Table 4 below. Only by reducing friendly dependence on UAS will the overall risk reduce.

	Medium (2 Points)	Friendly Dependence on UAS	**Total Risk**
Enemy EW/Cyber Capability	2	High (x3 Multiplier)	**18**
Enemy EW/Cyber Reach	2		
Enemy EW/Cyber Intent	2		
	1-12: Low Risk	13-17: Medium Risk	>17: High Risk

Table 4. Risk Matrix Results for Medium Ability and High Dependence

Another interesting scenario is that of peacetime operations near an adversary nation. State-level actors with high levels of capability and reach, but with a low intent to use also generate a high overall risk to Air Force operations that are highly dependent on UAS platforms. A practical example of this would be current US operations in the South China Sea area.[68] An intelligence assessment of China's EW/Cyber capabilities and reach would likely yield a medium to high rating, but with a low intent to employ them since the US and China are not actually at war. As shown in Table 5, this still yields a medium risk level during operations if the US is highly dependent on UAS for mission accomplishment. The risk would immediately transition to high as should the adversary decide to employ their EW/Cyber capabilities against friendly UAS.

	Medium (2 Points)	Friendly Dependence on UAS	**Total Risk**
Enemy EW/Cyber Capability	2	High (x3 Multiplier)	**15**
Enemy EW/Cyber Reach	2		
Enemy EW/Cyber Intent	1		
	1-12: Low Risk	13-17: Medium Risk	>17: High Risk

Table 5. Risk Matrix Results for Medium Ability, Low Intent, and High Dependence

RECOMMENDATIONS

From the three COAs explored above, it is clear that the risk level associated with operating UAS against an enemy with EW/Cyber capabilities is strongly associated with the level of dependence that friendly forces place on the UAS to accomplish critical mission objectives. A low dependence level generally produces the lowest level of risk regardless of an enemy's EW/Cyber ability, but since it ignores many of the inherent benefits of UAS operations – particularly the ability of some long-endurance UAS to loiter for extended periods of time near a battlefield – it is not the most preferable COA. A COA with a high dependence on UAS is also not the most preferable – with only a marginal increase in enemy capability or intent to use it, the overall mission is immediately put at a high risk level should the UAS be rendered ineffective.

The most preferable COA that remains is that of medium dependence of UAS systems for mission accomplishment. Based on the examples given above, this assessment is valid for multiple types of operations that the Air Force may be involved in. The most challenging scenario, however, is that of major contingency operations against a peer-level enemy capable of generating an A2/AD with EW/Cyber capabilities against friendly aircraft. In this MCO environment, considering a medium level of friendly dependence on UAS, friendly objectives are enhanced by the employment of UAS, but not wholly dependent on them. UAS with ELINT capabilities can help C2 identify enemy radar systems for destruction, while UAS with BACN equipment will help C2 distribute that information quickly to both strike assets for destruction and all other assets for threat warning. Importantly, to meet the goal of medium dependence, if the UAS assets listed above are rendered ineffective by an enemy's EW/Cyber weapons, the manned aircraft could still accomplish the overall mission objectives, though at a reduced level of effectiveness.

CONCLUSION

Referencing the COA outcomes and recommendations above, it is reasonable that adversary electronic warfare and cyber-attacks will pose a high level of risk to friendly mission accomplishment if operational objectives are highly dependent on UAS mission completion. To maintain a medium EW/Cyber risk level for UAS involvement in Air Force operations, the key term to remember is “desired, not required.” Unmanned assets have great abilities in the area of long endurance and relatively low cost; ignoring these benefits by leaving UAS out of a mission package solely to reduce risk would be leaving possible enhancements to nearly any military operation unused.

On the opposite end of the spectrum, relying too heavily on UAS to accomplish a desired mission against an enemy capable of effective EW/Cyber-attacks leads to a high risk level that is generally unacceptable. A medium dependence, considering the strengths, vulnerabilities, and employment of both manned platforms and UAS, would most often be the preferred way of fully leveraging the abilities of a UAS to give the best chance of accomplishing mission objectives.

The UAS EW/Cyber Risk Matrix provided above, or a similar product, is one tool that can provide commanders insight into the EW/Cyber aspect of mission risk regarding UAS. As described above, the matrix is intentionally open for interpretation by intelligence and operations personnel to provide overall assessments of enemy versus friendly systems. This provides flexibility to the risk assessment outcome, while also allowing for continuous assessment of the risk level as real-world operations progress and change.

NOTES

[1] Spencer Ackerman and Noah Shachtman, “Almost 1 In 3 U.S. Warplanes Is a Robot,” *Wired Danger Room*, January 9, 2012.

[2] United States Air Force. “RPA Vector: Vision and Enabling Concepts 2013–2038.” Headquarters, United States Air Force (17 February 2014): 14.

[3] Amber Corrin. “The Air Force's Anti-Access Area Denial Problem.” C4ISR & Networks (16 September 2015). http://www.c4isrnet.com/story/military-tech/isr/2015/09/15/air-force-anti-access-anti-denial/72317652/.

[4] United States Air Force. “RPA Vector:” 11.

[5] Bryan Krekel. “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.” Northrop Grumman Corporation (9 October 2009). http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf: 14-15.

[6] United States Air Force. “RPA Vector:” 32.

[7] Air Force Instruction (AFI) 90-802. *Risk Management*. Air Force Safety Center (23 March 2015). http://static.e-publishing.af.mil/production/1/af_se/publication/afi90-802/afi90-802.pdf

[8] Hartmann, Kim and Steup, Christoph. “The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment.” NATO Cooperative Cyber Defense Centre of Excellence Publications, 2013. https://ccdcoe.org/cycon/2013/proceedings/d3r2s2_hartmann.pdf: 3-4.

[9] Scott Peterson. “Iran Hijacked US Drone, Says Iranian Engineer.” Christian Science Monitor (15 December 2011). http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.

[10] Hartmann and Steup: 4.

[11] AFI 90-802: 16.

[12] Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. “Unmanned Systems Integrated Roadmap FY2011-2036.” Department of Defense (2011): v.

[13] Kris Osborn. “Navy Secretary Says Future Navy Fighter Planes Will Be Unmanned.” Military.com (16 April 2015). http://www.military.com/daily-news/2015/04/16/navy-secretary-says-future-navy-fighter-planes-will-be-unmanned.html.

[14] Hartmann and Steup: 4-8.

[15] United States Air Force. “RPA Vector:” 32.

[16] Ibid.

[17] Hartmann and Steup: 10-12.

[18] A.J. Kerns, D.P. Shepard, J.A. Bhatti, and T.E. Humphreys. "Unmanned Aircraft Capture and Control via GPS Spoofing." *Journal of Field Robotics*. 31(4): 617–636, 2014. http://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf.

[19] Air Force Policy Directive (AFPD) 90-8. *Environment, Safety and Occupational Health Management and Risk Management.* Air Force Safety Center (2 February 2012): 8-9.

[20] AFI 90-802: 3.

[21] AFI 90-802: 4.

[22] AFI 90-802: 12-13.

[23] AFI 90-802: 13-14.

[24] AFI 90-802: 15.

[25] AFPAM 90-803: 18.

[26] AFI 90-802: 16.

[27] Northrop Grumman. “RQ-4 Block 30 Global Hawk Datasheet.” Northrop Grumman Systems Corporation (2012). http://www.northropgrumman.com/Capabilities/GlobalHawk/Documents/Datasheet_GH_Block_30.pdf.

[28] Northrop Grumman. “RQ-4 Block 40 Global Hawk Datasheet.” Northrop Grumman Systems Corporation (2012). http://www.northropgrumman.com/Capabilities/GlobalHawk/Documents/Datasheet_GH_Block_40.pdf.

[29] Northrop Grumman. “Battlefield Airborne Communications Node.” http://www.northropgrumman.com/Capabilities/BACN/Pages/default.aspx (Accessed 24 August 2016).

[30] Northrop Grumman. “MQ-4C BAMS UAS Datasheet.” Northrop Grumman Systems Corporation (2011). http://www.northropgrumman.com/Capabilities/BAMSServiceSupportandTraining/Documents/pageDocs/bams.pdf.

[31] Northrop Grumman. “Q-4 Enterprise.” Northrop Grumman Systems Corporation (2012). http://www.northropgrumman.com/Capabilities/GlobalHawk/Documents/Brochure_Q4_HALE_Enterprise.pdf.

[32] Ibid.

[33] Ibid.

[34] Howell, Elizabeth. “Navstar: GPS Satellite Network.” Space.com (14 February 2013). http://www.space.com/19794-navstar.html.

[35] U.S. Naval Observatory. “Current GPS Constellation.” (Accessed 24 August 2016). http://tycho.usno.navy.mil/gpscurr.html.

[36] National Coordination Office for Space-Based Positioning, Navigation, and Timing. “Space Segment.” (Accessed 24 August 2016). http://www.gps.gov/systems/gps/space/.

[37] Howell.

[38] Department of Defense. “Global Positioning System Standard Positioning Service Performance Standard (4th Edition).” (September 2008). http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf: 4.

[39] Dunn, Michael J. “Navstar GPS Space Segment/User Segment L5 Interfaces.” Global Positioning Systems Directorate (24 September 2013). http://www.gps.gov/technical/icwg/IS-GPS-705D.pdf: 8.

[40] Shim, Elizabeth. “North Korea Sent 2,100 GPS Jamming Signals to South.” United Press International (29 June 2016). http://www.upi.com/Top_News/World-News/2016/06/29/North-Korea-sent-2100-GPS-jamming-signals-to-South/8211467212439/.

[41] Shim, Sun-ah. “N. Korea's Jamming of GPS Signals Poses New Threat: Defense Minister.” Yonhap News Agency (5 October 2010). http://english.yonhapnews.co.kr/national/2010/10/05/67/0301000000AEN20101005005900315F.HTML.

[42] Wesson, Kyle and Humphreys, Todd. "Unhackable Drones: The Challenges of Securely Integrating Unmanned Aircraft into the National Airspace." April 2013, draft submitted to *Scientific American*. http://radionavlab.ae.utexas.edu/images/stories/files/papers/unhackabledrones_for_distribution.pdf: 3.

[43] Kerns et al: 3.

[44] https://www.cl.cam.ac.uk/~mgk25/ih2004-navsec.pdf: 249-250.

[45] Kerns et al: 8.

[46] Hartmann and Steup: 1.

[47] Bartles, Chuck. “Russia’s Perspective on the Ways of Countering UAV Technologies.” *Operational Environment Watch* (Vol. 5 Issue 4, April 2015). Foreign Military Studies Office. http://fmso.leavenworth.army.mil/OEWatch/201504/201504.pdf: 53.

[48] McLeary, Paul. “Russia’s Winning the Electronic War.” *Foreign Policy* (21 October 2015). http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/.

[49] Concern Radio-Electronic Technologies. “Krasukha Deployed in Military Exercises.” (19 October 2015). http://www.kret.com/en/news/4027/.

[50] Concern Radio-Electronic Technologies. “Eastern Military District to Receive the New Krasukha.” (15 February 2015). http://www.kret.com/en/news/3656/.

[51] TASS News Agency. “Russia Developing System Capable of ‘Switching Off’ Foreign Military Satellites.” (25 June 2015). http://tass.ru/en/russia/803788.

[52] Concern Radio-Electronic Technologies. “Krasukha Delivered Ahead of Schedule to the Russian Army.” (9 October 2014). http://www.kret.com/en/news/3514/.

[53] TASS News Agency. “Foreign Buyers Interested in Russia’s Krasukha Electronic Warfare Systems – Company.” (26 August 2015). http://tass.ru/en/russia/816597.

[54] Heginbotham, Eric et al. “The U.S.-China Military Scorecard.” (RAND Corporation, Santa Monica, CA: 2015): 249.

[55] Protek. “Automated Complex Jamming P 330M1P Diabazol.” (Accessed 24 August 2016). http://www.protek-vrn.ru/production/avtomatizirovannyj-kompleks-radioelektronnogo-podavleniya-r-330m1p-diabazol/.

[56] McLeary.

[57] Perry, Bret. “How NATO Can Disrupt Russia’s New Way of War.” Defense One (3 March 2016). http://www.defenseone.com/ideas/2016/03/nato-russia-sof-ew-hybrid-war/126401/.

[58] Organization for Security and Co-operation in Europe. “Latest from OSCE Special Monitoring Mission to Ukraine.” (10 July 2015) http://www.osce.org/ukraine-smm/171821.

[59] Schiebel Corporation. “Camcopter S-100 Unmanned Air System.” (Accessed 24 August 2016). https://schiebel.net/products/camcopter-s-100-system-2/.

[60] Joint Chiefs of Staff. “Joint Operating Environment 2035.” (14 July 2016): 35

[61] Ibid.

[62] Krekel: 6-7.

[63] Krekel: 80.

[64] Heginbotham et al: 281-3.

[65] LeMay Center for Doctrine. “Annex 2-0 Global Integrated Intelligence, Surveillance & Reconnaissance Operations.” (29 January 2015).https://doctrine.af.mil/download.jsp?filename=2-0-D06-ISR-Intel-Prep-Op-Env.pdf.

[66] United States Air Force. “RPA Vector:” 54.

[67] Northrop Grumman. “Battlefield Airborne Communications Node.”

[68] Blanchard, Ben and Macfie, Nick. “U.S. Says Its Forces Will Keep Operating in South China Sea.” Reuters (20 July 2016). http://www.reuters.com/article/us-southchinasea-ruling-usa-idUSKCN1000PD.

BIBLIOGRAPHY

Air Force Instruction (AFI) 90-802. *Risk Management*. Air Force Safety Center (23 March 2015). http://static.e-publishing.af.mil/production/1/af_se/publication/afi90-802/afi90-802.pdf.

Air Force Policy Directive (AFPD) 90-8. *Environment, Safety and Occupational Health Management and Risk Management.* Air Force Safety Center (2 February 2012).

Bartles, Chuck. "Russia's Perspective on the Ways of Countering UAV Technologies." *Operational Environment Watch* (Vol. 5 Issue 4, April 2015). Foreign Military Studies Office. http://fmso.leavenworth.army.mil/OEWatch/201504/201504.pdf.

Department of Defense. "Global Positioning System Standard Positioning Service Performance Standard (4th Edition)." (September 2008). http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

Dunn, Michael J. "Navstar GPS Space Segment/User Segment L5 Interfaces." Global Positioning Systems Directorate (24 September 2013). http://www.gps.gov/technical/icwg/IS-GPS-705D.pdf.

Hartmann, Kim and Steup, Christoph. "The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment." NATO Cooperative Cyber Defense Centre of Excellence Publications, 2013. https://ccdcoe.org/cycon/2013/proceedings/d3r2s2_hartmann.pdf.

Heginbotham, Eric et al. "The U.S.-China Military Scorecard." (RAND Corporation, Santa Monica, CA: 2015): 249.

Joint Chiefs of Staff. "Joint Operating Environment 2035." (14 July 2016).

Kerns, A.J., Shepard, D.P., Bhatti, J.A., and Humphreys, T.E. "Unmanned Aircraft Capture and Control via GPS Spoofing." *Journal of Field Robotics*. 31(4): 617–636, 2014. http://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf.

Kim, Alan et al. "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles." American Institute of Aeronautics and Astronautics (no date). https://engineering.purdue.edu/HSL/uploads/papers/cybersecurity/cyber-attack-lit-review.pdf.

Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." Northrop Grumman Corporation (9 October 2009). http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

LeMay Center for Doctrine. "Annex 2-0 Global Integrated Intelligence, Surveillance & Reconnaissance Operations." (29 January 2015). https://doctrine.af.mil/download.jsp?filename=2-0-D06-ISR-Intel-Prep-Op-Env.pdf.

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. “Unmanned Systems Integrated Roadmap FY2011-2036.” Department of Defense (2011).

Tippenhauer, Nils Ole et al. “On the Requirements for Successful GPS Spoofing Attacks.” Swiss Federal Institute of Technology, (no date). http://www.cs.ox.ac.uk/files/6489/gps.pdf.

United States Air Force. “RPA Vector: Vision and Enabling Concepts 2013–2038.” Headquarters, United States Air Force (17 February 2014). http://www.af.mil/Portals/1/documents/news/USAFRPAVectorVisionandEnablingConcepts2013-2038.pdf.

Wesson, Kyle and Humphreys, Todd. "Unhackable Drones: The Challenges of Securely Integrating Unmanned Aircraft into the National Airspace." April 2013, draft submitted to *Scientific American*. http://radionavlab.ae.utexas.edu/images/stories/files/papers/unhackabledrones_for_distribution.pdf.

Yochim, Jaysen A. “The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack.” U.S. Army Command and General Staff College, 6 November 2010.