AN INVESTIGATION INTO THE INFORMATION REQUIREMENTS FOR REMOTELY PILOTED AIRCRAFT CREW WHEN DEALING WITH CYBER THREATS

Dr. Kristen K. Liggett
Air Force Research Laboratory
Dayton, OH
Mr. Peter Venero
CAMO, LLC
Dayton OH
Dr. Gina Thomas
Air Force Research Laboratory
Dayton OH

Remotely piloted aircraft (RPA) crews of the future will encounter more than the traditional threats to their aircraft. In addition to air-to-air and surface-to-air missiles, future conflicts will most likely include cyber weapons. While cyber weapons can certainly cause physical damage to these aircraft, the potential also exists to turn the friendly RPA against their own forces. The goal of the Resilient and Assured UAS Systems and Operations (RAUSO) program is to develop a cyber security module (CSM) that will detect and defend RPAs from cyber attacks. In some cases, the CSM will need to act automatically to defeat the threat. In other cases, the threat can be isolated and dealt with at an appropriate time in the mission. As powerful as the CSM will be, it will not be able to determine an appropriate time to address an attack. In order to maintain the best mission performance, the CSM will have to "negotiate" with the human crew as to when the appropriate time is to address an attack. A study was conducted to determine the most effective way to present relevant information to RPA crews to inform them of cyber attacks, courses of action, and mission impacts for successful negotiation of actions with the CSM. Five two-person crews (pilot and sensor operator) executed simulated missions, and data were collected to determine mission performance degradation under two levels of cyber attack and how that degradation was impacted by the CSM. Alerting improved performance for both levels of attack.

Over the past 15 years, the use of remotely piloted aircraft (RPA) to conduct Air Force missions has increased exponentially, and this trend is expected to continue into the future (USAF, 2014). RPAs are used effectively for intelligence, surveillance, and reconnaissance (ISR), tracking targets, and delivering weapons in a variety of missions. One of the biggest advantages of using RPAs is that the RPA operators can conduct dangerous missions without jeopardizing their lives because operators in safe locations (typically the US) communicate with the vehicles in theatre via a satellite connection. The arrangement of vehicle, operator ground control station (GCS), and satellite represents nodes in a network and may be vulnerable to cyber compromises/attacks. Also, the vehicle itself contains a network of line replaceable units connected to a 1553 bus, also susceptible to cyber attack. One of the biggest challenges facing our Air Force today is making the avionics of air assets resilient to cyber threats (Gross, 2016; Skowronski, 2016). Members of the Resilient and Assured UAS Systems and Operations (RAUSO) team are trying to develop a cyber security module (CSM) that will detect and defend RPAs from cyber attacks. From a human factors perspective, the challenge is determining how a new technology capable of detecting cyber events should behave to ensure that the RPA crew can sustain mission performance. Integral to that challenge is ensuring the RPA crew understands how they can leverage the information made available by the technology.

In preparation for this study, the researchers participated in a series of knowledge acquisition activities with RPA operators from Springfield Air National Guard (SPANG) and Syracuse Air National Guard (SANG). The goals were to better understand the RPA missions and to determine how operators regarded the potential threat of cyber attacks (Dukes, Fox, Rigrish, Durkee, & Feeney, 2016). Specifically, the researchers were hoping to better understand how crews develop and maintain their mental model of the cyber/RPA space. Surprisingly, RPA crews don't fully understand the RPA system vulnerabilities to cyber attacks. The team also determined methods crews currently use to handle traditional anomalies in emergency situations in order to study how those methods might change or need to change in cyber situations that are expected to be detected by the CSM. One of the objectives of this study was to expose operators to cyber threats to determine if they would recognize them as cyber threats without being alerted. The second objective was to determine effects of applying traditional alerting procedures on operators' mission effectiveness under cyber attack.

Method

Simulation Environment

The study was conducted using the Vigilant Spirit Control System (VSCS), an interface testbed with a virtual simulation capability (Feitshans, Rowe, Davis, Holland, & Berger, 2008). Three components of the VSCS were used for this study: a pilot control station, a sensor operator control station, and a simulation component that allowed the researchers to create ecologically-valid and repeatable mission scenarios. The scenarios were created in the VSCS virtual world and then executed for data collection. VSCS currently has alerts and checklists embedded in their system, which is modeled after the MQ-9 Block 50. The alerts and checklists developed for the cyber attacks had the same look and feel as other alerts and checklists. Figure 1 shows the sensor operator control station with a cyber checklist activated.

Figure 1. VSCS Sensor Operator Control Station [tactical situation display on the left monitor and checklist, sensor feed, and chat windows on the right monitor].

Mission Scenario

The basic scenario used for this study was a variation of a scenario created by MITRE (Dinsmore et al., 2015). The task started with the RPA in a loiter pattern around a building in a compound where the planning of nefarious activities was believed to be taking place. The crew was instructed to observe the building for people exiting, follow anyone leaving the building, and report the locations of activities they observed while following the vehicle. In the scenario, a man left the building and drove directly to another building believed to be a weapons cache. Then, he drove the vehicle to a second location, exited the vehicle and displayed signs of digging (as if planting an improvised explosive device [IED]).

During scenarios that contained a cyber attack, attacks could present in one of two ways. The first was a loss of the sensor ball feed (a low-sophistication attack). The second was an intentional drift of the sensor's global positioning system (GPS) coordinates (a high-sophistication attack). The low-sophistication attack would occur at the time when the man exited the building and drove away in a red truck, preventing the sensor operator from observing this activity. The high-sophistication attack was less obvious and resulted in the passing of inaccurate coordinates for the location of a weapons cache and the IED implantation. For the scenarios that had the CSM activated, when a cyber attack occurred, an alert was presented on both the pilot and sensor operator's screens describing the type of attack that was detected along with a checklist with instructions of how to remedy the problem. These types of RPA cyber vulnerabilities are consistent with the results of the USAF Scientific Advisory Board Report on Operating Next-Generation Remotely Piloted Aircraft for Irregular Warfare (Scientific Advisory Board, 2010).

Participants

Participants were recruited from SPANG. Based on availability, eight members of the guard and two former RPA operators who served as subject matter experts participated in the study for a total of five two-person

crews (pilot and sensor operator). The average RPA (MQ-1 Predator) flight hours for the pilots was 930 hours. The average experience of the sensor operators was 1572 total hours with an average of 1500 hours on the MQ-1.

Experimental Design

There were two independent variables in this study: two levels of CSM (active and not active) and two levels of sophistication of cyber attack (low-sophistication and high-sophistication) for a total of four conditions in a full-factorial within-subjects design. The dependent variable was a compiled measure of the crew's successful detection of a person leaving the building and accurately reporting the truck's location and the locations of the weapons cache and the IED implantation. In order to control for any learning effect, the initial location of the loiter pattern, the route the truck took to the second building, and the location of second building and the IED implantation was varied in the five scenario runs.

Procedure

Participants were greeted, and the purpose of the study was explained. They were given a short demographic questionnaire, a briefing about the details of the study, and were trained on VSCS. All crews performed an initial scenario with no cyber attacks to establish baseline performance. Then, all crews performed two missions with the CSM not present; one with a low-sophistication attack and one with a high-sophistication attack. Since the CSM was not present for these two conditions, the crew had no alert or checklists for resolving the problems. The order of these conditions was balanced across the five crews. After completing the missions without the CSM active, the crew performed two missions with a cyber threat present and the CSM active. Again (separately), the order of these two conditions was balanced across the five crews. Following data collection, crews were asked a series of questions to provide further insight into current operations and how cyber information should be presented in the future.

Results

The purposes of this initial study were to determine if there were practical effects of alerting crews to cyber intrusions and to ascertain an approximation of the size of expected effects for future research planning. It should be noted that there were no statistically significant effects found, which is not surprising due to the lack of statistical power resultant from the very low number of subjects (low N so effect size would have to be extremely large to show statistical significance).

When no cyber attack was present, crews, on average, were able to perform 95% of the tasks in the mission, but when a cyber attack was present without the CSM, crews completed only 25% of mission tasks. However, adding the CSM brought task completion back up to 83% (Figure 2). There appears to be a slight interaction between the presence of CSM and the type of attack (Figure 3). Crews were generally better at performing their tasks under drift than when the screen went blank regardless of whether or not CSM was present.

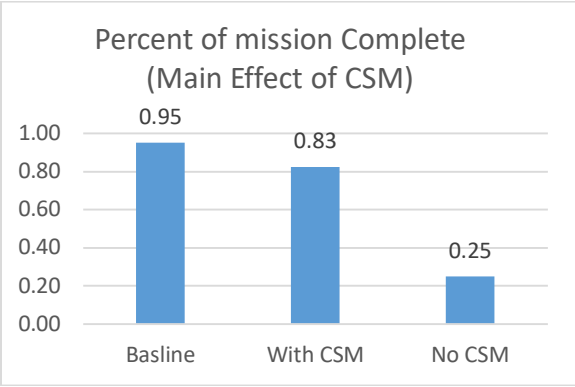


Figure 2. Effect of CSM.

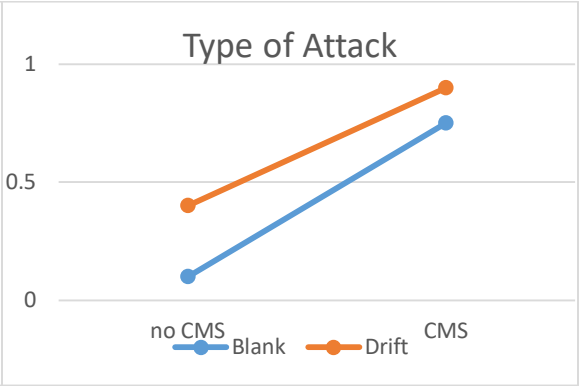


Figure 3. Use of CSM by Type of Cyber Attack.

Although the presence of the CSM improved performance in both attack conditions, CSM appeared to provide a bit more of a boost to performance in the blank condition, perhaps due to there being more room for improvement. Results of subsequent discussions with the crew members are addressed in the discussion.

Discussion

The effects of having the CSM active confirmed expectations that a system that would alert the crew of a cyber-based problem would result in better performance. The lower performance on the low-sophistication threat (sensor ball blanking) occurred because of a combination of the sensor ball setting and the rules of engagement that the crews were following. Crews were instructed to loiter over a building and watch for anyone leaving the building. The low-sophistication attack occurred when the person left the building, so when the sensor ball came back up, if the sensor operator had it zoomed in, they missed the person leaving the building. If they maintained their rules of engagement (stay loitering until you observe a person leaving) they would not zoom out and search for the red truck unless instructed to do so (by the customer in the real world or the experimenter in the study), so they missed the rest of the mission events. Note that accuracy was not 0% when the CSM was not active because some of the sensor operators had the sensor zoomed out to a level such that when the sensor feed came back on, they could still see the red truck leaving the compound and follow it. For the high-sophistication cyber threat (GPS coordinates drift), participants could complete the first two objectives (watch for a person and follow the truck) regardless of the attack but the coordinates they passed for the location of the weapons cache and the IED implantation would be incorrect when the CSM was not active. Therefore, any difference in performance (more improvement for low-sophistication attack) is probably due to having more room for improvement in the low-sophistication attack condition.

In terms of the crew-member feedback, much information was obtained regarding how the RPA crews go about dealing with emergencies and maintaining their mental models throughout these situations. Figure 4 shows the state space of possible alignments between the operator's mental model and the actual state of the system. Clearly the goal is to have the crews' mental model aligned with the current state of the world (shown in green). When there is a mismatch between the actual state and the operator's mental model (shown in pink), two things can result: 1) operators don't recognize a problem, or 2) they spend time on a problem that doesn't exist. Both of these situations lead to decreased mission effectiveness. When the operators think things are normal, they seem to be employing a more passive scan pattern, simply consuming key pieces of information that verify this situation. The crew does not seem to actively cross-check multiple sources of information against expected values to make sure they all indicate that the plane is, in fact, in a normal state. In other words, it is only when something unexpected and relatively obvious happens (i.e., an alert activates) that the crew detects the abnormal state and they subsequently seek out information that is not readily apparent. So one way in which alerting improves performance is that it provides that unexpected event causing the operator to move from the incorrect state of believing an abnormal system is normal to the correct state of believing the abnormal system is abnormal, minimizing the time spent in the incorrect state.

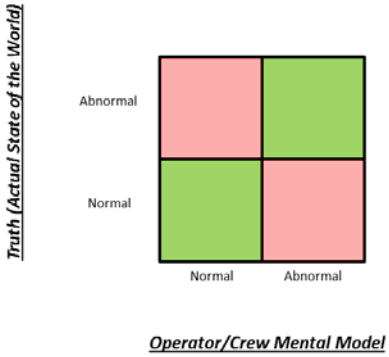
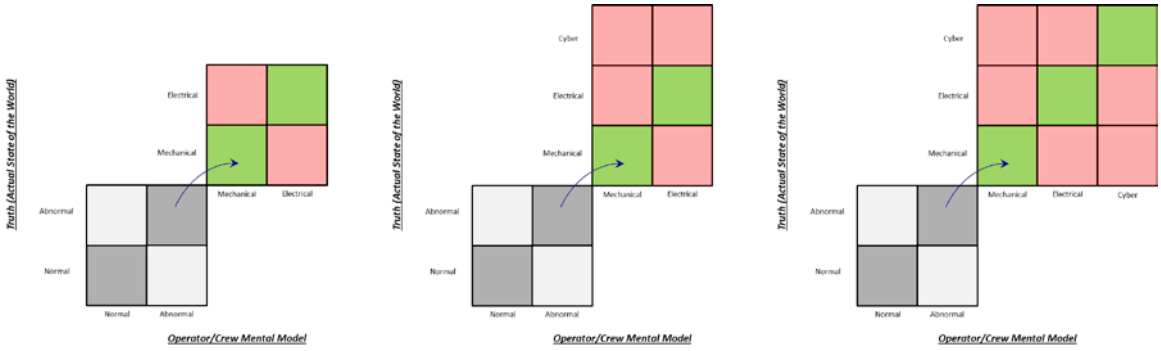


Figure 4. Actual State and Operator Mental Model Space.

Figure 5a expands the abnormal/abnormal state by showing this space with traditional mechanical and electrical failures. Figure 5b represents the current state of affairs in which a cyber attack is a possible cause of the abnormal state, but the operator's mental model about potential causes of abnormal states has not updated to include

cyber attacks. In this case, when a cyber attack happens, the operator's understanding about the cause of the problem will always be incorrect. Figure 5c shows the possible conditions once operators are made aware of the potential for cyber attack. In this case, there is at least a chance that the operator will correctly identify the cause of the abnormality. In post-trial interviews, experimenters learned that some alerts cause multiple checklists to appear. When operators were asked how they decided which checklist to follow, they indicated that the one they chose was based on experience, but what they described was a process of looking at various information elements to determine which path to go down. This shows a shift in their procedure when an alert is present – from passive scanning of available information to actively seeking information relevant to the situation. The green boxes in figure 5c show the goal, which is to align the operator's mental model of possible abnormalities with the actual cause.



(a) (b) (c)

Figure 5. Actual State and Mental Model Abnormal Situations.

In the case of a cyber attack, the ability of the operator to shift from normal to abnormal relies on the CSM accurately detecting cyber events and providing e the additional information elements necessary for the operators to determine what course of action to take. These requirements for CSM are being fed back to the technology developers in the RAUSO program to ensure maximum benefits may be provided by the CSM.

Unfortunately, cyber events can occur for which providing an alert to the operator is not possible as some attacks are subtle and stealthy. How can the operator move quickly from normal/normal to abnormal/abnormal cyber when no alert is present? Recall from earlier in the discussion, the hypothesis is that operators in the normal/normal state are using a more passive reasoning method to maintain their awareness of the actual state of the system and, thus, are typically not actively cross-checking information against expected information for multiple sources but are instead fitting observed information into their definition of normal. This method will likely cause them to miss an unalerted cyber event that does not cause an obvious change in system behavior. Operating in this new environment requires imparting knowledge of various potential cyber threats and how those events would likely manifest themselves to the crew. The challenge will be in getting operators to change their reasoning approach. Another alternative is to design new interfaces that highlight the information elements necessary for crews to understand the situation in such a way that they can readily perceive mismatches in the case of cyber attack, allowing them to process the information in a way. The design of such interfaces is a challenge for future research, but raising awareness that cyber events are possible, describing how those could manifest themselves during a mission, and alerting operators to detectable cyber events is a good first step.

.

Conclusion

This study provides a significant first step in understanding how RPA operators need to receive information about cyber attacks in order to maintain mission effectiveness. Clearly, the best situation is to have a CSM that can detect the type of threat and provide information on how best to respond. Integrating cyber alerts and checklists into the standard format for mechanical and electrical alerts and checklists provides a sense familiarity for the operators when dealing with these new types of threats. However, in the future, new interfaces will need to be designed so operators can cross-check multiple sources of information quickly and efficiently so they can also detect and appropriately respond to cyber attacks that have gone undetected by the CSM.

Acknowledgements

We would like to acknowledge Dr. Steven King from ASD(R&E) for supporting the RAUSO program, Mr. Herb Mullens for providing programming support, and the Vigilant Spirit Control Station Team in 711 HPW/RHCI; specifically Greg Feitshans, Jason Davis, Jimmy Whelan, and Mark Squire.

References

Dinsmore, M., Jella, C., Lewis, M., Neal, D., Rush, J., Gay, C., Horowitz, B., Lau, N., and Leach, K. (2015). Developing cyber security CONOPS for remotely piloted aircraft (RPA) missions. *MITRE Technical Report 150032*, Bedford, MA: The MITRE Corporation.

Dukes, A. W., Fox, O. M., Rigrish, R. N., Durkee, K. T., and Feeney, J. J. (2016). *Resilient & Assured UAS Systems & Operations (RAUSO) Hybrid Cognitive Task Analysis*. (Air Force Research Laboratory Publication). Wright-Patterson AFB, OH: Author.

Feitshans, G. L., Rowe, A. J., Davis, J. E., Holland, M., & Berger, L. (2008). Vigilant spirit control station (VSCS) "The face of COUNTER". *AIAA Guidance, Navigation and Control Conference and Exhibit*, 1-12. doi: 10.2514/6.2008-6309

Gross, C. (2016). AFMC commander says cyber threats are real, need to get ahead of them. *USAF News and Information*. Washington DC: USAF. Retrieved from http://www.af.mil/News/ArticleDisplay/tabid/223/Article/951715/afmc-commander-says-cyber-threats-are-real-need-to-get-ahead-of-them.aspx

Scientific Advisory Board. (2010). *Operating Next-Generation Remotely Piloted Aircraft for Irregular Warfare*. SAB-TR-10-03, Washington DC: Author. Retrieved from https://publicintelligence.net/usaf-drones-in-irregular-warfare/

Skowronski, W. (2016). Vulnerability in cyberspace. Air Force Magazine, November/December, 52-53. Retrieved from http://www.airforcemag.com/MagazineArchive/Magazine Documents/2016/November 2016/1116cyber.pdf

United States Air Force. (2014). *RPA Vector: Vision and Enabling Concepts 2013-2038.* Washington DC: Author.