Contract AI Risk Engine (CARE) to Reduce Cyber Contracting Risk

Major Y. Brian Lee Major Dennis Kim Major Wallace Rollins

INTRODUCTION

he Fiscal Year 2019 National Defense Authorization Act (NDAA) established the National Security Commission on Artificial Intelligence (NSCAI) to consider the methods and means necessary to advance development of artificial intelligence (AI), machine learning (ML), and other associated technologies to address America's national security concerns. NSCAI's final report to the President and Congress identified areas of weakness that the federal government must address to elevate data security as a national security priority. NSCAI recommended the federal government implement a security development lifecycle approach for AI systems, prioritize data privacy and security considerations as part of larger efforts to strengthen foreign investment screening and supply chain intelligence and risk management, and integrate national security considerations into efforts to legislate and regulate data protection and privacy.¹

Current Department of Defense (DoD) information technology (IT) contracting policies, vehicles, and practices lack definitive language or terms that give due process to national security considerations. Without contracting language specifically tailored to the cyber security threats facing the United States (US), DoD cannot adequately secure the DoD Information Network (DODIN) nor protect it from foreign influence. Contractual languages often favor the vendor. For example, DoD cyber vendors can potentially circumvent DoD prohibited IT equipment or prevent DoD Cyber Protection Teams from inspection or damage assessment during cyber breaches or attacks, citing ambiguous contracting language and proprietary corporate intellectual protection as justifications.² Unfortunately, contracting personnel, commanders, and staffs across the DoD lack training and expertise in

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



Major Y. Brian Lee, U.S. Army, is a Medical Service Corps officer assigned to the Department of Defense Chief Digital and Artificial Intelligence Office, Arlington, VA. He holds a BA from Washington University in St. Louis, a MS from the University of Maryland Global Campus, and a Masters in Operational Studies from the U.S. Army Command and General Staff College. During his career, MAJ Lee served with the Joint Artificial Intelligence Center, 7th Special Forces Group, 2nd Infantry Division, 82nd Airborne Division, and 65th Medical Brigade.

reducing cyber security risk. An objective cyber contract risk score does not exist. DoD should leverage ML in the cyber contract requirements generation process to reduce cyber contract risk and position DoD to better prevent, monitor, and respond to cyber threats.

Issue

Contracts for cyber or IT related products and services present a cyber supply chain risk for the DoD. Cyber supply chain risk stems from a lack of visibility into, understanding of, and control over many of the processes and decisions involved in the development and delivery of cyber products to the Joint Force.³

Requirement owners and contract management offices are at the forefront of cyber supply chain risk management (C-SCRM). As the requiring activity, commanders and their staff determine and develop requirements and generate the performance work statement (PWS). Contracting officers, vested with the authority to obligate the US government to legally binding contracts, coordinate and finalize contracting actions to provide the goods or services needed by the requiring activity. Unfortunately, requiring activities and contracting professionals often lack the technical expertise to articulate specific C-SCRM measures within contracts. Further, existing resources that provide guidelines and standards for C-SCRM are inadequate with respect to the granular process of contract writing and are spread across a multitude of DoD policies (Figure 1).

Publications from the National Institute of Standards and Technology (NIST), Defense Acquisition University (DAU), and DoD Instruction documents describe how to conduct C-SCRM, but no publication goes into more nuanced details on contract language, thus creating gaps in cyber supply chains. Current acquisition processes account for various risks, but in-depth technical understanding of the cyber supply chain is required to properly translate mitigation measures into contract language during the requirements generation process.



Major Dennis Kim, U.S. Army, is a Medical Service Corps officer assigned to 65th Medical Brigade, Camp Humphreys, Republic of Korea. He holds a BS from Boston University, an MBA from The College of William and Mary, and a Masters in Operational Studies from the U.S. Army Command and General Staff College. During his career, MAJ Kim served with the 10th Mountain Division, and Infantry Division, and the U.S. Army Medical Materiel Agency.

During a lecture at the U.S. Army Command and General Staff College in April 2021, Brigadier General (BG) Paul Craft, Commandant of the U.S. Army Cyber School, used the cloud migration of Army data as an opportunity to address both the benefits and challenges that data contracting presents. BG Craft acknowledged it is unrealistic to expect all contracting officers to be cyber security experts, but a lack of understanding of cyber security can lead to inadequate language in contracts. This has led to instances where data became lost, mishandled, or the DoD denied access to its own data and required to pay to get data back. BG Craft cautioned that this situation can be especially damaging when there is a breach, and the language of the contract does not authorize DoD Cyber Protection Teams to investigate the breach. This lack of transparency and access erodes the public trust and harms national security.

APPROACH AND SOLUTION

This proposal recommends the use of AI through ML to review draft contracts uploaded by contracting officers and analyze the cyber security risk to the DoD. After review, the Contract AI Risk Engine (CARE) produces recommended clauses most advantageous to DoD for cyber security along with a cyber risk level which measures the level of risk to DoD for the contract as written. The requiring activity reviews the recommendations and adjusts the contract as necessary. The contracting officer subsequently takes the improved contract and obtains a new risk score, with scores above a certain threshold requiring command concurrence by both the requiring activity commander and the supporting contracting commander before moving to contract fulfillment. As a pilot, CARE recommendations are initially based upon the Army Contracting Command's (ACC) repository of previous IT and cyber related contracts. Upon successful testing, the intent will be to incorporate a Joint solution and include data from all services and DoD agencies. CARE relies upon cloud computing and AI platforms, such as the DoD's Advana enterprise



Major Wallace Rollins, U.S. Army, is an Acquisition Corps officer assigned to Program Executive Office Soldier, Fort Belvoir, VA. He holds a BA from Virginia Polytechnic and State University, an MBA from the University of Kansas, and a Masters in Operational Studies from the U.S. Army Command and General Staff College. During his career, MAJ Rollins served with the 82nd Airborne Division, 3rd U.S. Infantry Regiment, "The Old Guard," the 1st Cavalry Division, and 1st Security Force Assistance Brigade.

analytics platform, for data analysis, model generation, and risk score calculation.

Artificial Intelligence Design

Contracting affects DoD agencies and activities, the military services, and Combatant Commands. Using CARE to reduce cyber contracting risk is a feasible ML project with immediate real-world applications and implications where end users can see the benefits of augmenting contracting processes with AI. DoD has partnered with national academic research institutions, such as the MIT Lincoln Laboratory and the Army's AI Task Force at Carnegie Mellon University, to accelerate the research and development of national security AI priorities. While partnerships and national conversations on the research, development, and applications of AI advance the state of DoD AI initiatives, Soldiers, Airmen, and Sailors have yet to experience the transformational benefits promised by AI in daily operations. Incorporating AI into the Joint Force will create a generational shift in how business is conducted. For commanders to champion AI and for the end user to experience the benefits of AI, DoD must bridge the crisis of trust between humans and AI, whether that AI is operating in autonomous-capable weapons systems or as software platforms.⁵ Building trust requires repetitive exposure through the rapid development and implementation of small-scale projects rather than conceptual projects that will not mature for years to come. Quick wins that create buy-in from the operational force will advance the state of DoD AL

The human-machine relationship should be carefully considered when designing AI projects and use cases. Requirement developers and AI practitioners determine the degree of autonomy granted to each AI product. The three degrees of autonomy are commonly referred to as human-in-the-loop, human-on-the-loop, and humanout-of-the-loop. In human-in-the-loop (HITL) operations, the machine performs a task and waits for the human

BRIAN LEE : DENNIS KIM : WALLACE ROLLINS

Cybersecurity-Related Policies and Issuances Developed by the DoD Deputy Cit for Cybersecurity Last Update: Jane 24, 2022 Send genetication in Control Control Cybersecurity													
				ORGAN	NZE								
·				Lead and G	Bovern								
Interim National Security Strategic Guidance	2022 National Defense Stategy (NDS)	National Military Brategy (NMS) (0	19 National Intelligence Strategy	National Cyber Strategy Na	idional Strategy to Secure 53 Nation	Cyberspace U.S. Hr1 St	utegy for Cyberspace Information 31	ligence Community 2018 DoD Cy naming Strategy	ber Strategy				
D/D Dyal Modernation Strategy DuD Operatively RNA Productions DUD Operatively													
ORGANIZE		ENABLE		ANTICIPATE		PREPARE		AUTHORITIES					
Design for the Fight		Secure Data in Transit		Understand the Battlespace		Develop and Maintain Trust		Title 10, US Code Armed Forces (862224, 3013/b), 5013/b), 5013/b);	Tife 14, US Code Cooperation With Other Agencies (Ch. 7)				
NIST SP 803-119 Guidelines for the Secure Deployment of IPv6	CNSSP-11 Nat1 Palicy Governing the Acquisition of IA and IA-Enabled IT	FIPS 140-3 Security Requirements for Cryptographic Modules	NIST SP 802-153 Guidelines for Securing Wireless Local Acea Networks	FIPS 193 Standards for Security Categorizatio of Federal Info. and Info. Systems	NIST SP 800-59 Guideline for identifying an Information System as a NSS	CNSSP-12 National IA Policy for Space Systems Used to Support NSS	CNSSP-21 National IA Policy on Enterprise Architectures for NSS	Title 32, US Code National Guard (\$102)	Title 40, US Code Public Buildings, Property, and Works (Cite 113: 6511302 11315 11331)				
CNSS National Secret Fabric Architecture Recommendations	DFARS Subpart 208.74, Enterprise Software Agreements	CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material	CN3SP-15 Use of Pub Standards for Secure Sharing of Info Among NSS	NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info an Info Systems to Security Categories	d Guide to Computer Security Log Nanagement	NIST 803-160, vol.1. Systems Security Engineering Engineering of Trustworthy Secure Systems	CNSSI-5002, Telephony Isolation Used for Unified Comme, Implementations w/ in Physically Protected Spaces	Title 44, US Code Federal Information Security Mod. Act.	Title 50. US Code War and National Defense				
DaDD C-5100.19 (CAC He(d) Critical Information Communications (CRITCOM) System	D-sDD 5200.47E Arti-Tamper (AT)	CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info	CNSSP-19 National Policy Governing the Use of HAIPE Products	NISTIR 7593 Specification for Asset Identification	ChSSD-320 1.5 Use of Mobile Devices to Process Nat1 Sec.Info Outside Secure Spaces	DaDD 3020.40 Mission Assurance	DeDD 3100.10 Space Policy	Clinger-Cohen Act, Pub. L. 104-106	UCP Unified Command Plan				
DoDO 7045.20 Capability Portfolio Management	DoDD 8115.01 IT Portfolio Management	CNSSP-25 National Policy for IKI in National Security Systems Communications		CNSSP-28 DoDI 5-5240.23 Cyberscourty of Unmarned National Security Systems Cyberspace		Strengthen Cyber Readiness		NATIONAL	/ FEDERAL				
DuDI 5000.02 Operation of the Adaptive Acquisition Framework	DaDi 5030.07 Operation of the Software Acquisition Pathway	Communications Security (COM/SEC) End Item Modification End Item Modification		Prevent and Delay Attackers and Prevent Attackers from Staying		NIST SP 600-207 Zero Trust Architecture	NIST SP 800-18, R1 Guide for Developing Security Plana for Federal Information Systems	Computer Fraud and Abuse Act Title 18 (§1030)	Federal Wretap Act Title 18 (§2510 et seq.)				
DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN	DoDI 7000.14 Finanoial Management Policy and Procedures (PPDE)	Type-Acceptance Program for VolP Telephones	Natl COMSEC Instruction Protection of Govit Contractor Telecomm's DoDD 8100.02	FIPS 200 Minimum Security Requirements for Federal Information Systems	NIST SP 800-37 R2 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems	NIST SP 000-00, R1 Guide for Conducting Risk Assessments	NIST SP 800-39 Managing Information Security Risk	Stored Communications Act Title 18 (§2701 et seq.)	Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)				
DoDI 81 15.02 IT Portfolio Management Implementation	DoDI 83 10.01 Information Technology Standards in the DoD	CNSSI-7033 Protected Distribution Systems (PDS)	Use of Commercial Wintless Devices, Services, and Tech in the DoD GH3 DoD14650.01	NIST SP 800-53 R5 Security & Privacy Controls for Federal Information Systems	NIST SP 803-53A R5 Assessing Security & Privacy Controls in Fed. Into. Systems & Orgs.	NIST SP 800-126, R3 SCAP Ver. 1.3	NIST SP 1000-25 Data Integrity: Identifying and Protecting Assets Against Ransomvare	Poteign Intelligence Surveillance Act Title 50 (§1801 et seq)	Executive Order 13231 as Amended by EO 13286 - Critical Infrastructure Protection in the Info Age				
DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)	DaDI 85 10.01 Rak Management Framework for DoD IT	Department of Defense Dometrics De01 8100.04	Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum Ds018420.01	NIST SP 800-61, R2 Computer Security Incident Handling Guide	NIST SP 800-124, R1 Guidelines for Managing the Security of Mobile Devices in the Enterprise	NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government	CNSSP-32 Cloud Security for National Security Systems	Executive Order 13528 Classified National Security Information	Executive Order 13597 Structural Reforms To Improve Classified Nets				
DeDI 8580.1 Information Assurance (IA) in the Defense Acquisition System	RMF Knowledge Service	DoD Unified Capabilities (UC) DoDI 8523.01	Commercial WLAN Devices, systems, and Technologies DeDI 5-0200.16 Objectives and Min. State by COMISEC	N ST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems	NIST SP 800-163, R1 Vetting the Security of Mobile Applications	CNSSD-505 Supply Chain Risk Management	CNSSD-520 The Use of Noble Devices to Process National Security Information Outside	Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing	EO 13638: Improving Critical Infrastructure Cyberse curity				
MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Listensing Agreements	DODAF (Version 2.02) DeD Architecture Framework	CUCS/ 6510.02E	Measures used in NC2 Comms C-/CS/ 6519.06C Communications Security Releases to	NIST SP 1800-26 Data Integrity: Detecting & Respondin to Ransomware	ChSSI-1011 Implementing Host-Based Security Casebilities on NSS	DaDD Strott of Control (C2) Enabling Capabilities	National Leadership Command Capability	ED 13800: Strengthening Cybersecurity of Fed Nets and Cl	NSD 42. National Policy for the Security of Nat'l Security Telecom and Information Systems				
DTM 20-004 Enabling Cyberspace Accountability of DoD Components and Information Systems	Common Criteria Evaluation and Validation Scheme (CGEVS)	Citypeographic Modernization Plan Manage	Paneige Nations	CNSSI-1013 Network Intrusion Detection Sys & Intrusion Prevention Sys (IDS/IPS)	CN55I-1253 Security Categorization and Control Selection for har1 Security Systems	And Reporting of Cybenspace Workforce Requirements	United Platform and Joint Cyber Command and Control (JCC2)	EO 13873: Securing the Information and Communications Technology and Services Supply Chain	EO 14028: Improving the Nation's Cybersecurity				
CJCSI 5123.01H Charter of the JROC and Implementation of the JCID	Joint Publication 6-0 Joint Communications System	HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors	PIPS 201-3 Personal Identity Verification (PI//) of Federal Employees and Contractors	CNSSI-1253F, Atchs 1-5 Security Overlays	CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS	DoDI 8500.01 Cybersecurity	DeDI 8560.01 COMSEC Monitoring	IISPD 54 / IISPD 22 Computer Security and Monitoring	PPD 21: Critical Infrastructure Security and Resilience				
Develop the Workforce		NIST SP 800-210 General Access Control Guidance for Cloud Systems	NIST SP 1900-16 Securing Web Transactore: TLS Server Certificate Management	DoDI 5000.00, Cyberneoutly for Acquisition Decision Authorities and Program Managers	DeDI 5200.39 CPI Identification and Protection within RDT&E	Sustain Missions NIST SP 800-34, R1 NIST SP 800-82, R2		PPD 41: United States Cyber Incident Coordination	PPD 28, Signals Intelligence Activities				
NBT SP 800-181 R1 Workforce Framework for Cyberseoutly	NSTISSD-501 National Training Program for INFOSEC Professionals	CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information	CNSSP-10 Nat'l Policy Gov. Use of Approved Sec. Containers in Info Security Applications	DoD Is205.83 DoD Insider Threat and Managemen and Analysis Center	DaDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations	Federal Information Systems CASSIP-18	Guide to Industrial Control Systems (ICS) Security	FAR Federal Acquisition Regulation	A-130, Management of Fed Info Resources				
CNISSD-504 Protecting National Security Systems from Insider Threat	CNSSD-600 Communications Security Monitoring	CNSSP-16 National Policy for the Destruction of COMISE C Paper Material	CNSSP-200 National Policy on Controlled Access Protection	DoD18531.01, DoD Vulnerability Management	DeDI 8551.01 Ports. Protocels, and Services Management (PPSM)	Netlonal Policy on Classified Information Spillage CNSSIF-300	Policy for National Security Systems CNSS/-N01	Ethics Regulations	Joint Special Access Program (SAP) Implementation Guide (JSIG)				
CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment	NSTISSI-4011 National Training Standard for INFOSEC Professionals	National Directive for ICAM Capabilities .	National Directive to Implement PKI on Securit Networks	DeD 0-8530.1-M (CAC reg(d) CND Service Provider Certification an Accreditation Program	nd DoDM 5105 21V1, SCI Admin Security Manual: Info and Info Sys Security	Comproming Emanators CMSS-4004.1. Destruction and	Information Spillage CNSSI-0007	NIST Special Publication 800-Series	NIST SP 800-63 series Digital identity Guidelines				
CNSSI-4012 National IA Training Standard for Senior Systems Managers	CNSSI-4013 National IA: Training Standard For System Administrations (SA)	CN55I-1303 Instructions for NSS PKI X 509	Operational Society Doctine for the PORTEZZA User PONCIA Card	DTM: 17-007. Ch. 2. Defense Support to Cyber Incident Response Corputer Network Defense (CND)		COMSEC and Class. Material CNSSI-7600 TEMPEST Countierroad was for	Utility Program	NGT SP 800-88, R1,Guidelines for Media Sanitzation	NIST SP 800-101, R1 Guidelines on Mobile Device Forensios				
CN381-4014 National W Training Standard For Information Systems Security Officers	National Training Standard for System Certifiers	CNSSI-6001 Controlled Cryptographic Items CNSSI-6005	Reporting and Evaluating CONSEC Incidents	CJCSM 6510.018 Cyber Incident Handling Program	CJCSM 6510.02 IA Vuinerability Mgt Program	Facilities De0D 3020.28	De0D 3020.44	NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms	NET SP 800-137 Continuous Monitoring				
CNSSI-40.16 National IA Training Standard For Risk Analysts	DeDD 8140.01 Cyberspace Workforce Management	Safeguarding COMSEC Pacilities and Materials, amended by CNSS-008-14 DeDI 1000.25	Controlling Authorities for CONISEC National DeDI 5200.01	ABOUT THIS CHART		DeDD 5144.02	DoDD 8000.01 Management of the DOD information	NIST SP 000-209 Security Guidelines for Stonage Infrastructure	NISTIR 7250, R3, Glossary of Key Information Security Terms				
DeDM 3305.09 Cryptologic Accreditation and Certification	DeD 8570.01-M Information Assurance Workforce Improvement Program	DoD Personnel Identity Protection (PIP) Program DoDI 5250.08	DaD Information Security Program and Protection of SCI DoDI 5200.48	 Insistent organizes cyteneseurry policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key), Double-clicking" on the box directs users to the most authoritative publicly accessible source. Bohima in italian calculate the document is measured for licensity directs in the source. 		DoDi 5000 83 Technology & Program Protection to	Enterprise DeDI 6410.02 NetOps for the Global Information	CNSSD-602 National Directive On Security of National Security Systems	CNSSD-901 Nat'l Security Telecomm's and info Sys Security (CNSS) Issuance System				
Partner for Strength		Resources and the DoD PSRB DeDI 8520.02	Lonrosed Utdassifed Information(CU) DeDI 0520.03	 no authoritative public-facing hy The linked sites are not controls 	perink is currently available. ed by the developers of this chart. We	Maintain Technological Advantage ICD 503	Grid (013) UEC 4.010-00.	CNSSD-900, Governing Procedures of the Committee on National Security Systems	CNSSI-4009 Crite on National Security Systems Glossary				
NET SP 802-144 Quidelines on Security and Privacy in Public Claud Competition Public Claud Competition		Public Key Intrastructure (PKI) and Public Key (PK) Enabling	Identity Authentication for Information Systems	regularly check the integrity of th experience an error message di decision to move the document.	he links, but you may occasionally ue to problems at the source site or the site's . Please let us know if you believe the link is	17 Systems Security Risk Management and C&A NSA /A Directorate ((AD) Management	Cybersecutty of Facility-Related Control Systems	DeD Information Technology Environment Strategic Plan					
NIST SP 800-172A Enhanced Security Requirements for National Policy Governing the Release		DeDM 1000.13, Vol. 1 DeD ID Cards: ID Card Life-syste Program Manual		no longer valid. CNSS policies link only to the CNSS site. Provide with only to the CNSS site.		Diversive MD-310 Cryptographic Key Protection	Program Protection	OPERATIONAL ISUBORDINATE POLYON					
Protecting CUI of 1A Products Services CNSSI-4008 DoDI 5205.13		Assure Information Sharing		 Note: It is best to open this PDF directly in a browser. However, if you are unable to open the links directly from this PDF document, place your oursor 		C	Rey-CPRs	- Littlin About					
Program for the Mgt and Use of Nat1 Reserve IA Security Equipment DoDM 0-5205.12	Defense Industrial Base (DIB) Cyber Security (CS) / IA Activities Da0 5220 22-M, Ch. 2	CNSSP-24 Policy on Assured Into Sharing (A/S) for National Security Systems(NSS)	DoDI 8170.01 Online Information Management and Electronic Messaging	over the target box and right-click to copy the link location. Open a web browser and paste the copied link into the address bar. For the latest version of this chart or email alerts to updates go to <u>https://</u>		000 CO	NEA USD(%8)	CYSERCOW Orders Security Configuration Guides	JHO-DODW Orders				
Classification Marcual Crassification Marcual	Operating Manual (NISPON) NOA Between DoD and DHS	DoDI 8320.02 Sharing Data, Info. and IT Services in the DoD	DoDI 8582.01 Security of Non-DoD Info Sys Processing Unslassified Nonpublic DoD Monwation	dodae.dto.mildod.oybersecurit	a, pang, chatt	DA1	CYNERICOM Other Agencies USDUARS) Process pericy activity updated pericy	(503)	Mercarende) Security Technical Implementation				
Certification (CNINC)	(Jan. 19, 2017)	CJCSI 3213.01D. Joint Operations Security	CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities	Distribution Statement A: Distribution is unlimited.	Approved for Public Release.	(1 mo	LBD(C) Explod, Lpdok pending	Risk to Galilleer	Guildes (STIGs)				

Figure 1. Cybersecurity policies and issuances for the DoD.⁴

user to take an action.⁶ In human-on-the-loop (HOTL) operations, the machine decides and acts on its own, but a human user supervises its operations and can intervene if necessary.⁷ In human-out-of-the-loop (HOOTL) operations, the machine decides and acts on its own, and the human user cannot intervene in a timely fashion.⁸ The risk associated with the degrees of autonomy vary and should be carefully weighed based on the intended applications of the machine, the chances of faulty actions to occur, and the severity caused by faulty actions. Given that the purpose of this project is to reduce the risk associated with DoD cyber and IT contracting, we propose that AI recommended contracting clauses and risk determination require HITL acceptance both in modifying contracting language during the contract support process as well as involving commanders to accept contracts of considerable risk with or without language modification. Once implemented, CARE augments, rather than replaces, the human decision-making process.

To develop DoD end user trust in AI, CARE does not remove human involvement and instead harnesses the efficiency of intelligent automation to best inform the human decision-maker.⁹ Trust builds as users throughout the contracting chain see tangible benefits from CARE-assisted contracting compared to the standard human-only contracting process.

ML requires data to improve model performance. DoD contracts in document format cannot provide the necessary data to begin training ML algorithms. Natural language processors combined with numerical scoring of contract features must be developed, and contract scoring does not currently exist. Feature engineering is the determination of the appropriate data variables necessary for ML algorithms to assess what the user requires.¹⁰ In other words, poor feature engineering results in subpar model performance. Prior to any data collection for CARE development, DoD contract stakeholders throughout the contracting process with proper AI education must carefully determine the features that will create the contracting data necessary for ML algorithms to work and with the least amount of data bias (Figure 2).

Contract Num	Туре	Unit Type	Cost	Feature 1	Feature 2	Feature 3
2020.02.01	Hardware	Tactical	\$5,002	5	2	4
2020.02.02	Software	Service	\$22,678	2	3	2
2020.02.03	Hardware	CCMD	\$540,555	5	1	1
2020.02.04	Hardware	CCMD	\$874,322	3	5	5
2020.02.05	Software	Operational	\$54,178	1	3	3

Figure 2. Feature engineering example

Development and Operational Concept

In a case study on Army contracting analytic capabilities, the RAND Corporation piloted an effort to make unstructured historical contract data machine readable to forecast a contract's likelihood to have unliquidated obligations.¹¹ We propose to utilize similar methodologies as RAND in accessing and scoring cyber and IT contracts over a set number of fiscal years with the inclusion of contract performance and contract closeout reports. Contracts would be analyzed by trained cyber and contracting experts and scored on features developed during feature engineering for the data. We seek to score cyber and IT specific contractual language in a tabular format. Proposed feature categories include, but are not limited to, contract duration, contract language, contract outcome, contract performance, adversarial incursion, DoD cyber response, and contract barriers. Close collaboration with data scientists during contract scoring will reduce introducing biased data into the dataset. While RAND utilized over 300,000 contracts with 150 features over three fiscal years, we are unsure how many Army-specific cyber and IT contracts exist at this time.¹² A period of discovery should be included in the CARE development timeline.

Upon completion of contract scoring, developers perform exploratory data analysis to ensure quality data, build and work with predictive models, evaluate models and receive predictions, and refine outputs. CARE determines a contract's risk to DoD and outputs a risk percentage and recommended changes to reduce the risk. A lower risk means that the contract's language provides DoD with favorable execution outcomes. A higher risk percentage suggests that DoD will potentially meet resistance from contractors in response to adverse security events. CARE will recommend specific contractual language modifications and inform end users where that language should go in the contract. Users explore how CARE recommended modifications af-

BRIAN LEE : DENNIS KIM : WALLACE ROLLINS

fect risk, whereby as modifications are selected in the user interface, the contract would be reassessed and the net result displayed in a live risk meter. Users could choose all recommendations or select recommendations, with selections based on the requiring activity's desired combination of potential cost, time, and scope as considerations for risk acceptance. As a HITL system, CARE must rely upon the contracting officer to accept modifications. Cyber and IT contracts continue to be generated by requiring activities, and CARE will be further refined in the future as new data, including CARE augmented contracts, are introduced into the model.

CARE would be a web-portal ML platform with a file upload and document review user interface (Figure 3). Contracting officers upload draft contracts for analysis and interact with recommendations for decision-making analysis only. To reduce the cost and complexity of developing and maintaining CARE, contracting officers transfer recommendations manually into the original document creation software, most likely Microsoft Word or Adobe Acrobat, prior to contract fulfillment. CARE is decision augmentation only. Contracting officers should consult with the requiring activity before accepting any CARE modifications, and risk scores above a certain percentage would require both the requiring activity and contracting commanders to concur. CARE enables commanders to analyze risk, considering risk to the force and risk to the mission against the perceived benefit of the contract.¹³





Based upon current development timelines from ML projects being piloted at U.S. Army Forces Command (FORSCOM), we believe that CARE can be rapidly developed with the involvement of data scientists, contract specialists, and cyber security experts in under three months (Figure 4) utilizing the collaborative framework of DevSecOps and agile delivery. We anticipate an additional six to nine months to complete Authorization-To-Operate (ATO) requirements as necessary, working through ML Ops challenges to deploy and maintain models reliably in the production environment, user interface design, and policy decisions. By developing a narrow scope that precisely targets the problem that CARE solves, DoD can responsibly and rapidly prototype and field a platform that decreases contracting risk with immediate and tangible benefits. However, we do acknowledge the risk of the "valley of death" that a successful model development does not guarantee inclusion into a program of record for further sustainment and adoption.



Figure 4. Projected CARE development timeline

CONCLUSION

Cyber-attacks by foreign adversaries and criminal organizations have revealed how the American people and the economy rely on the cyberspace domain. As more DoD operations migrate to the cloud with as-a-service contracting and as DoD activities contract for capabilities to enable a competitive edge in training and in combat, reducing the cybersecurity risk of these contracts is paramount for DoD to defend against and respond to adversarial cyber operations. We recommend that the U.S. Army Materiel Command, assisted by, in coordination with, and potentially developed through the DoD Chief Digital and Artificial Intelligence Office (CDAO), funds and develops CARE. Upon successful pilot testing, it would mandate all cyber and IT contracts to adopt CARE as a critical component in the contract approval process. DoD cannot allow contracting language to cripple America's national security interests. Developing and implementing CARE for DoD cyber contracting will create a more resilient DoD cyber supply chain with the necessary contractual safeguards for DoD to prevent, monitor, and respond to cyber and IT related adversarial events.

BRIAN LEE : DENNIS KIM : WALLACE ROLLINS

NOTES

- 1. National Security Commission on Artificial Intelligence, Final Report: National Security Commission on Artificial Intelligence (Washington, DC, 2021), 50.
- 2. Paul G. Craft, personal communication, April 20, 2021.
- 3. National Institute of Standards and Technology, Information and Communications Technology Supply Chain Risk Management, (Washington, DC: Department of Commerce, 2021), https://csrc.nist.gov/CSRC/media/Projects/Sup-ply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf.
- 4. "Build and Operate a Trusted DoDIN," Defense Technical Information Center, 2022, https://dodiac.dtic.mil/wp-content/uploads/2022/07/2022-06-24-csiac-dod-cybersecurity-policy-chart.pdf.
- Dan G. Cox, "Artificial Intelligence and Multi-Domain Operations: A Whole-of-Nation Approach to Success," *Military Review*, 101, no. 3 (May-June 2021): 76-91, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MJ-21/MJ21-Whole-Book-2.pdf.
- 6. Paul Scharre, Army of None (New York: Norton, 2018), 29.
- 7. Ibid., 29.
- 8. Ibid., 30.
- 9. Ge Wang, "Humans in the Loop: The Design of Interactive AI Systems," Stanford University, 2019, https://hai.stanford. edu/news/humans-loop-design-interactive-ai-systems.
- 10. "Feature Engineering," DataRobot, 2021, https://www.datarobot.com/wiki/feature-engineering/.
- William Marcellino et al., Army Analytic Capabilities: A Case Study Within Army Contracting Command and Its Implications, RR-A106-1 (Santa Monica, CA: Rand, 2021), 1, https://www.rand.org/pubs/research_reports/RRA106-1.html.
- 12. Ibid., 5.
- 13. Department of the Army, Mission Command: Command and Control of Army Forces, ADP 6-0 (Washington, DC: Department of the Army, 2019), 1-13.