Managing Cybersecurity Research and Experimental Development: The REVO Approach

Dan Craigen, Drew Vandeth, and D'Arcy Walsh

> *"No one means all he says, and yet very few say all they mean, for words are slippery and thought is viscous."*
>
> Henry Adams (1838–1918)
> Journalist, historian, academic, and novelist

We present a systematic approach for managing a research and experimental development cybersecurity program that must be responsive to continuously evolving cybersecurity, and other, operational concerns. The approach will be of interest to research-program managers, academe, corporate leads, government leads, chief information officers, chief technology officers, and social and technology policy analysts. The approach is compatible with international standards and procedures published by the Organisation for Economic Co-operation and Development (OECD) and the Treasury Board of Canada Secretariat (TBS). The key benefits of the approach are the following: i) the breadth of the overall (cybersecurity) space is described; ii) depth statements about specific (cybersecurity) challenges are articulated and mapped to the breadth of the problem; iii) specific (cybersecurity) initiatives that have been resourced through funding or personnel are tracked and linked to specific challenges; and iv) progress is assessed through key performance indicators.

Although we present examples from cybersecurity, the method may be transferred to other domains. We have found the approach to be rigorous yet adaptive to change; it challenges an organization to be explicit about the nature of its research and experimental development in a manner that fosters alignment with evolving business priorities, knowledge transfer, and partner engagement.

Introduction

In many academic, private, or public contexts, research programs must address critical challenges and produce innovative discoveries. In addition, these discoveries often must be efficiently and effectively transformed into technological capabilities. Research programs that are continuously adaptive to business, technical, legal, and other drivers or constraints can enable the vitality and relevancy of research and experimental development (R&ED). Adaptive research programs can play a critical role in ensuring that major or minor scientific or technological breakthroughs respond to evolving operational environments.

In this article, we present the Research in Evolution (REVO) approach for managing a research program that we employ to address cybersecurity-related concerns. At its core, REVO is based upon distinguishing what R&ED needs to be done from what R&ED is being done. The method is intentionally compatible with the standards from the Organisation for Economic Co-operation and Development (OECD; oecd.org) and the Treasury Board of Canada Secretariat (TBS; tbs-sct.gc.ca) that provide guidance about the scope of such programs, related definitions, and performance indicators. The method is rigorous enough to enable (on-demand) reporting on scientific expenditures and personnel with respect to research, experimental de-

Managing Cybersecurity Research and Experimental Development: REVO Approach

Dan Craigen, Drew Vandeth, and D'Arcy Walsh

velopment, and related scientific activities as defined by the OECD.

REVO is not just a vehicle for producing reports. The method challenges researchers, related scientific-activity analysts, and research-program managers to be sufficiently explicit about the problem space and the solution space to enable the continuous re-alignment of scientific or technological investigations based upon a collective understanding of what should be done. Importantly, REVO accommodates innovation and accidental discovery through a decision-making (feedback) cycle. The intent of the REVO decision-making cycle is to ensure a research program is responsive to its operational environment by enabling discovery and harnessing those discoveries that matter. At all times, REVO-related information is managed in an integrated manner, even if selected information is not connected or is contradictory.

The specific objective of this article is to provide a concise but comprehensive review of the REVO method using an example from the cybersecurity domain to demonstrate the utility of the approach. We plan to further refine the approach as our understanding deepens and our experience grows.

In the first section of this article, we describe how strategic research contexts and research-requirement statements are used to articulate what needs to be done. In the second section, we describe how research-activity descriptions are used to track what is being done (including when providing information for Statistics Canada's Federal Scientific Expenditure and Personnel [FSEP; tinyurl.com/l9j2p22] survey). In the third section, we describe the lifecycle of the research program and explain how key performance indicators and a decision-making cycle are used when assessing the overall progress with R&ED. The cybersecurity example that is used throughout this article to illustrate the REVO approach is directly linked to the research focus area "Investigate practical enterprise-level metrics" described in the companion article by Craigen, Walsh, and Whyte (2013; timreview.ca/article/704).

Articulating What Needs To Be Done

In this section, we summarize the components of REVO used for describing the key challenges that drive our R&ED program. The first sub-section presents the notion of strategic research contexts, which we view to compose the breadth of our problem space. The second sub-section presents the notion of research-requirement statements, which are structured expressions of specific problems, and which we view to compose the depth of our problem space. We have found it useful to be able to: i) concisely summarize the challenge space overall; ii) separately describe specific problems in a fine grained and focused way; and iii) link these tightly scoped statements to a broader scope. When analyzing the link(s) that may exist from a specific research-requirement statement to one or more strategic research contexts, it becomes clear why the requirement is relevant with respect to the overall research program. When analyzing the link(s) that may exist from a particular strategic research context to one or more research-requirement statements, it becomes clear how well that aspect of the problem domain is understood and what specific research-related activities should be pursued.

Strategic research contexts

Strategic research contexts (SRCs) compose the breadth of our cybersecurity problem space. SRCs further explicate portions of our cybersecurity challenges and therefore inform the coverage of research requirements and alignment of research programs and activities. Based on our experiences with cybersecurity and discussions with other stakeholders in the domain, we have identified 19 SRCs that provide structure to the problem space (Box 1). We believe that research advances in these contexts will help achieve a stable and resilient information technology infrastructure for Canada.

Research-requirement statements

In the REVO process, the information technology department of the company's cybersecurity manager specifies what is needed using a template for a research-requirement statement. A simplified example of a completed research-requirement statement is provided in Appendix A (tinyurl.com/n6vkm82) using data from a fictitious enterprise. The example focuses upon a requirement for well-founded security measures and metrics. Though simplified here, the topic is a valid cybersecurity research requirement.

A research-requirement statement consists of 10 sections:

Section 1. Identification/Criticality: consists of basic information including date, identification number, a title, point of contact, and group, urgency and importance. In our example, we note that the requirement is urgent and of high importance to the enterprise (from the perspective of the business line).

Managing Cybersecurity Research and Experimental Development: REVO Approach

Dan Craigen, Drew Vandeth, and D'Arcy Walsh

Box 1. Strategic research contexts for cybersecurity

SRC1 – Mission Management
Comprises policy, priority, resource, and risk management in support of optimizing mission effectiveness.

SRC2 – Computational Platforms
Comprises forms of computation systems as a means of implementing particular types of algorithms, satisfying operational constraints, managing computation resources, and includes the application of specific approaches of interest.

SRC3 – Autonomous and Adaptive Systems
These are systems that are designed to respond automatically and without intervention to some range of environmental or operating conditions. Communities of heterogeneous or homogeneous systems can interact cooperatively among themselves and with the environment, or possibly dynamically reconfigure themselves, to meet a set of common mission goals.

SRC4 – Human–Computer Interaction
Includes all logical and physical forms of interface between humans and computers. Varieties of interaction are needed to suit the types of complex and voluminous mission information that humans must interpret and manipulate.

SRC5 – Sensor Architecture
Situational awareness and intelligent network management for cybersecurity require sensor architectures that identify host-based and network-based events and may enrich both situational awareness and network management by performing host-based, network-based, or combined analytics. Such architectures may require complex command and control capabilities.

SRC6 – Database Systems
Data must be represented, stored, manipulated, filtered, and retrieved to suit particular mission purposes and conditions.

SRC7 – Secure System Architecture
A set of system attributes, described in design artifacts, that specify how they relate to the overall IT architecture. These controls serve the purpose of maintaining the system's quality attributes, among them confidentiality, integrity, availability, accountability, and assurance.

SRC8 – Cryptanalysis
Used to characterize systems and to characterize vulnerabilities in encryption methods to access encrypted information. Methods can be mathematical, protocol based, or based on the physical-system implementation.

SRC9 – Computer Network Analysis
Used to characterize networks and to characterize vulnerabilities in networks that may be used to disrupt intended network functionality. A broad class of methods, drawing upon interdisciplinary techniques, must be understood for protecting modern cybersystems.

SRC10 – Trusted Computing
Provides the means to create trustworthy computational systems in environments that cross security domains. Trusted computing includes evaluation of expected software and hardware function and acceptable deployed risk of vulnerability; it also includes the development of methods of detecting, mitigating, and preventing compromises of system security. Trusted computing depends on techniques for constructing systems that are inherently secure at some level.

SRC11 – Computer Network Defence
Develop techniques to detect, assess, and respond to cyberintrusions of networks and systems. Computer network defence is informed by elements such as sensor architectures, computer network analysis, security measures and metrics, and knowledge discovery.

SRC12 – Security Measures and Metrics
Provide a quantitative and objective basis for security assurance, with the main uses being for strategic support, quality assurance, and tactical oversight. Metrics can be applied to measure the maturity of security processes or of the security posture.

SRC13 – Secure Communications
The creation of systems that allow two parties to communicate in a way that is insusceptible to eavesdropping or interception.

Continued on next page...

Managing Cybersecurity Research and Experimental Development: REVO Approach

Dan Craigen, Drew Vandeth, and D'Arcy Walsh

Box 1. (*continued*) Strategic research contexts for cybersecurity

SRC14 – Knowledge Discovery
An interdisciplinary field focusing on methodologies for extracting useful knowledge from data, drawing upon statistics, databases, pattern recognition, machine learning, data visualization, optimization, and high-performance computing. Knowledge discovery includes the efficient preparation, display, summarization, search, and filtering of complex data sets.

SRC15 – Distributed Computational Space
Development of analysis, filtering, retrieval, and other processing techniques for operating in a distributed computational environment either by their inherently distributed nature or distributed by constraint.

SRC16 – Advancing Analytics
Techniques for advanced logical analysis of data and human behaviour for a mission purpose, supporting an analytic process to make it more efficient, to make it more effective, to manage it, and to automate it. Data may be of large scale and from disparate sources, requiring different methodologies for understanding it.

SRC17 – Systems Engineering
The robust approach to the design, creation, and operations of systems. Systems engineering includes the specifying of system goals as well as articulating design concepts, tradeoffs, implementation, and verification.

SRC18 – Material Science
The application of advanced materials and fabrication techniques to enable other technologies and to support mission systems.

SRC19 – Cyber–Physical Systems (CPS)
Those systems in which there is a strong connection between computational (cyber) and physical elements. Much of our critical Infrastructure depends upon cyber–physical systems. Human-in-the-loop cyber–physical systems are those systems that consist of a human, an embedded system, and the physical environment. Human-in-the-loop systems can restore fundamental autonomy for functionally weakened individuals. A robust cyber-security framework will encourage deployment of cyber–physical systems, including human-in-the-loop systems.

Section 2. Stakeholders: the key operational stakeholders are identified. Normally, an operational stakeholder, a technical stakeholder and a subject-matter expert. In our example, we identified "Information Operations" and "Enterprise Security" as enterprise stakeholders and Mike Smith and John Doe as two subject matter experts.

Section 3. Business Description: here, the business motivations for the research requirement are captured. We give three example motivations in Appendix A, including the observation that it has become increasingly difficult to choose amongst security options because the benefits, costs, and tradeoffs are poorly understood.

Section 4. Research Requirement: the specifics of the research requirement are captured in this section, including technical challenges and proposed solutions or approaches. In our example, we observe that advancing the state of scientifically sound security measures and metrics would greatly aid the design, implementation, and operation of secure information systems.

Section 5. Success/Completion Criteria: often overlooked is a statement of how one knows that a research requirement has been resolved. Security measures and metrics are sufficiently immature that it is difficult to fully identify success. However, we would hope to ensure that: i) the security posture is continuously monitored; ii) the measurements meaningfully reflected security posture; and iii) both manual and automated responses to appropriate classes of threats are suitably informed.

Section 6. Category Impact: this refers to potential impact either to the enterprise, partners, or general enterprise research capabilities. The impact is low, medium, or high. In our example, the research is expected to have a high impact on the enterprise's operational capabilities.

Section 7. Description of Impact: reasons are provided for claims of a particular impact. For the example, we believe that enhanced understanding of the IT infrastructure will identify attack vectors and vulnerabilities and will better inform what system data is required.

Managing Cybersecurity Research and Experimental Development: REVO Approach

Dan Craigen, Drew Vandeth, and D'Arcy Walsh

Section 8. Relationship to Strategic Research Contexts: the depth of the requirement is tied to the breadth of the strategic research contexts. In this case, the link is particularly simple because the research requirement maps to SRC12: Security Measures and Metrics.

Section 9. Partnerships: researchers that we could leverage or partner with in advancing the requirement. In our example, we point to three institutions in the United States that are working in the area of "science of security" and have identified security measures and metrics as a hard challenge.

Section 10. Notes: a free-form section for any addition information the business line wishes to provide.

Assessing the research requirements

Based upon information at hand and guidance from the business lines, the requirements are categorized as advancing enterprise operational capabilities, advancing partner operational capabilities, or advancing enterprise research capabilities. Within these categories, research requirements are then tiered into three levels of enterprise criticality, with Tier I being the most critical.

Assessing the tier of a research requirement is based on the following five criteria:

1. Coverage of the strategic research contexts

2. Importance or impact within its category

3. Originator criticality specification (intra-research-requirement statement)

4. Other research-requirement statements (inter-research-requirement statement)

5. Retrospective information (heuristics, lessons learned)

Based on the resulting tier, the following requirements/focus areas are recommended:

1. Tier I requirements: should address critical internal-research issues; should be specified in a manner that is actionable by internal research capacity; are usually more granular and narrower in scope; and should be owned by a business-line research effort.

2. Tier II requirements: should supplement or augment internal research issues; should be specified in a manner that is actionable by internal research capacity, but primarily to drive the investigations of external research capacity to address the broader context; are usually more coarse grained and broader in scope; and should be owned by a business-line research effort.

3. Tier III requirements/focus areas: should be identified to drive predictive analysis investigations to supplement Tier I and Tier II investigations. (A research focus area, for example simulation techniques, identifies a general technical area of potential interest.)

Based on our experiences, we identified the following three options for applying appropriate resources:

1. Utilize internal research capacity

2. Form and manage external research relationships

3. Use predictive-analysis methods and techniques

In general, we recommend that, because of the breadth and depth of the problem space and the often-limited internal research capacity of the organization, such capacity should be focused on Tier I problems. Hence, for a Tier I requirement, we suggest that an optimal combination of the three resources be applied. For Tier II, a combination of external research relationships and predictive-analysis methods and techniques is optimal. For Tier III, predictive-analysis methods and techniques are appropriate. Optimization of resources should be determined on a case-by-case basis depending upon, for instance, organizational capacity, partnerships and funding.

Tracking What Is Being Done

In this section, we summarize the components of REVO that are used for specifying and tracking specific research endeavours that are planned, that are in progress, or that have been completed. In the following sub-section, we present the notion of research-activity descriptions and describe how they are aggregated to respond to the annual Federal Science Expenditures and Personnel (FSEP; tinyurl.com/l9j2p22) survey.

Research-activity descriptions

Research-activity descriptions are structured descriptions of specific internal or external investigations that have established resourcing levels in terms of expenditures or personnel. A specific research-activity description is linked to one or more research-requirement statements. When analyzing the link(s) that may exist from a specific research requirement statement to one

Managing Cybersecurity Research and Experimental Development: REVO Approach

Dan Craigen, Drew Vandeth, and D'Arcy Walsh

or more research-activity descriptions, it becomes clear what level of effort is required, including an indication of what degree of progress may be anticipated. When analyzing the link(s) that may exist from a specific research-activity description to one or more research-requirement statements, it becomes clear what impact the specific activity may have, or not have, depending upon the outcome of the particular investigation.

A simplified example of a completed research-activity description pertaining to security measures and metrics is provided in Appendix B (tinyurl.com/kzee5mj). A research-activity description consists of two parts:

Part 1: General information: consists of basic information such as fiscal year, point of contacts, and linkage to strategic research contexts.

Part 2: Research-activity information: consists of eight sections that provide particulars of the project. These sections are:

Section A. Project identification: further elaborates basic project information including a statement of the purpose of their work and the kind of work (experimental development or advancement of scientific knowledge). Depending upon the response, either Section B or Section C will be completed.

Section B. Experimental development: determines what technological advancements are being targeted, what technological obstacles exist, and what work has been directed at overcoming the obstacles. In our ongoing example, we discuss collecting known measures and metrics into a single compendium and then experimenting using an in-house enterprise laboratory. We state that the main obstacle is the identification of measurements and metrics of suitable quality. The uncertainty of the work is noted by the explicit statement that the work is sufficiently immature that it is unclear how the technical obstacles will be overcome.

Section C. Basic or applied research: though this section was not completed in our example, it determines what scientific knowledge is being progressed, what work is to be performed, and how it contributed to the scientific knowledge.

Section D. Additional project information: identifies the collateral developed by the project, such as planning documents, resource allocation, notebooks, and contracts.

Section E. Intramural expenditures: essentially captures internal expenditures.

Section F. Extramural expenditures: essentially captures external expenditures.

Section G. Personnel: determines how many individuals (measured as full-time equivalents) worked on the project or supported the project.

Section H. Sources of funds: determines where the funds come from.

Note that Sections E through H of the research-activity description provide the project's specific financial and staffing figures for the FSEP survey. The organization's response to FSEP will aggregate the figures from all of their R&ED projects.

Research Program Lifecycle

In this section, we summarize the components of REVO used to manage the research program lifecycle as a whole to ensure R&ED efforts result in required operational capability in an efficient and effective manner. We first present the key performance indicators (KPIs; tinyurl.com/ltsjzja) that are used to set targets (through establishing thresholds) and assess progress. Then, we present the decision-making cycle that is used to (re)align the research program when adapting to changing business, technical, legal, and other drivers or constraints.

Key performance indicators

The following four KPIs enable the full lifecycle of our R&ED program to be continually (re)assessed with respect to established and emerging research priorities. When other components of REVO change, the KPIs are recomputed. We believe they are useful high-level indicators that can apply to any domain under investigation.

KPI1. Alignment of research-requirement statements and strategic research contexts: provides a top-level indication of how well the breadth of the problem space is covered by research-requirement statements. This KPI is computed by setting thresholds for each strategic research context relating to the percentage of research requirements that are expected to be linked to that context. This dashboard-like indicator "goes red" when one or more strategic research contexts lack actionable problem statements.

Managing Cybersecurity Research and Experimental Development: REVO Approach

Dan Craigen, Drew Vandeth, and D'Arcy Walsh

KPI2. Balance of internal and external investigations: provides a top-level indication of how well balanced internal and external investigations are given internal resources. Ideally, internal capacity should only be used to address Tier I research requirements. This dashboard-like indicator "goes red" when internal resources are directed at research requirements that should ideally be addressed by external resources.

KPI3. Distribution of expenditures and personnel resourcing levels: provides a top-level indication of the distribution of research-related resources with respect to Tier I, Tier II, and Tier III research requirements. This KPI is computed by setting thresholds for each tier relating to the percentage of resources that are expected to be allocated to that tier. This dashboard-like indicator "goes red" when a particular tier is underfunded to the benefit of another tier.

KPI4. Assessment of progress of activities: provides a top-level indication of the progress of the research program as a whole with respect to the completion criteria that were specified for each research-requirement statement. This KPI is an aggregated result of assessments made by subject-matter experts about whether limited progress (0), high-potential progress (1), or definite progress (2) is being made for each active research initiative. This dashboard-like indicator "goes red" when the research program is not producing results effectively or efficiently.

The decision-making cycle

In this sub-section, we describe the high-level decision-making cycle that is used to keep the research program as a whole responsive to changing operational priorities. The research-program executive sets direction by validating the strategic research contexts and setting the thresholds that are used to compute KPIs. Subject-matter experts are responsible for articulating research-requirement statements and assessing progress of particular investigations. Research managers are responsible for tracking research activities that are part of their portfolio. When one or more indicators "turn red", decisions are taken to turn the indicator(s) back to green. Depending upon the indicator, this may mean:

- readjusting the representation of the strategic research contexts
- adding, deleting, or refining research-requirement statements
- changing the mapping between strategic research contexts and research-requirement statements
- adding, deleting, or refining research-activity descriptions
- changing the mapping between research-requirement statements and research-activity descriptions
- adjusting resource levels with respect to Tier I, Tier II, and Tier III research requirements
- adjusting thresholds

Conclusion

In this article, we have presented a high-level description of REVO using a specific cybersecurity requirement and activity description that are linked to the breadth of the cryptologic problem space. The examples are intended to illuminate the key artifacts that we have found give REVO its power as a practical and flexible systematic approach for managing R&ED. Due to time and space limitations, we have not been able to provide complete examples nor to report upon refinements specific to our work context. As our understanding deepens and our experience grows, we plan to publish more in-depth articles about how REVO enables us to address the cybersecurity context, principles, and focus areas described in the companion article by Craigen, Walsh, and Whyte (2013; timreview.ca/article/704).

We conclude by making comments about: i) the use of specific methods to address specific problems and ii) the use of a general methodology for a unified response to a large and complex R&ED challenge.

Use specific methods to address specific problems

Based upon our academic work and our ongoing investigations in the workplace, we understand that it is important to: i) have a clear and well-scoped understanding of the specific problem under investigation and ii) be explicit about the particular methodological approach that will be applied when pursuing an investigation. The methods applied should be "as strong as possible" in the sense that some methods may be more applicable than other methods, depending on the problem.

We advocate always specifying the particular methodological approach that will be adopted, coupled with the

Managing Cybersecurity Research and Experimental Development: REVO Approach

Dan Craigen, Drew Vandeth, and D'Arcy Walsh

description of the specific problem of concern. As an investigation proceeds, the methodology should be evaluated along with reporting any research results with respect to the problem itself.

Use a general methodology for a unified response to the challenge

We also recognize the need for applying a general methodology to facilitate a unified response to the challenge overall. In our view, this methodology needs to be "strong enough". A unifying method must balance rigour with flexibility. The general method must be rigorous enough to provide traceability to top-down and bottom-up objectives, including the quantification of performance metrics for R&ED. The method must also be flexible enough to accommodate the potentially highly divergent approaches that could be trialed on a problem-by-problem basis.

The general methodology should be well-informed by the definitions and methodologies pertaining to R&ED as espoused by the OECD's Frascati Manual (tinyurl.com/kq44wqx) for measuring scientific and technological activities.

Appendices

A. Example Research-Requirement Statement
Available online at: tinyurl.com/n6vkm82

B. Example Research-Activity Description
Available online at: tinyurl.com/kzee5mj

About the Authors

Dan Craigen is a Science Advisor at the Communications Security Establishment Canada (CSEC). Previously, he was President of ORA Canada, a company that focused on High Assurance/Formal Methods and distributed its technology to over 60 countries. His research interests include formal methods, the science of cybersecurity, and technology transfer. He was the chair of two NATO research task groups pertaining to validation, verification, and certification of embedded systems and high-assurance technologies. He received his BScH in Math and his MSc in Math from Carleton University in Ottawa, Canada.

Drew Vandeth is the Senior Research Strategist for the National Security Community and a Senior Researcher at IBM Systems Research. He is the founder of the Tutte Institute for Mathematics and Computing (TIMC) and was its first Deputy Director. His research interests include theoretical and computational number theory, contextual and cognitive computing, high performance computing architectures, autonomic and autonomous analytical systems, and research management. Dr. Vandeth holds a PhD in Number Theory from Macquarie University in Sydney, Australia, an MMath in Number Theory from the University of Waterloo, Canada, and a BMath (Hons) in Pure Mathematics, also from the University of Waterloo.

D'Arcy Walsh is a Science Advisor at the Communications Security Establishment Canada (CSEC). His research interests include software-engineering methods and techniques that support the development and deployment of dynamic systems, including dynamic languages, dynamic configuration, context-aware systems, and autonomic and autonomous systems. He received his BAH from Queen's University in Kingston, Canada, and he received his BCS, his MCS, and his PhD in Computer Science from Carleton University in Ottawa, Canada.

Citation: Craigen, D., D. Vandeth, and D. Walsh. 2013. Managing Cybersecurity Research and Experimental Development. *Technology Innovation Management Review*. July 2013: 34–41.

Keywords: cybersecurity, research, experimental development, performance indicators, strategic research contexts, research-requirement statements, research-activity descriptions, research program lifecycle