**Open Source Intelligence Tech Research Project**

# Objective

The purpose of this Open Source Intelligence (OSINT) Project is to use publicly available sources of information to investigate an emerging application of technology and then prepare a report suitable for dissemination to interested parties in business and government (subscribers to a threat intelligence reporting service).

# Overview

Your task is to develop an OSINT report which provides information about the characteristics of an emerging application of technology and the threats / attacks to which it may be vulnerable. The consumers of this report have an interest in developing suitable countermeasures to prevent attacks by a broad spectrum of attackers from hobbyists to quasi-professionals and criminal entities to well organized, nation-state sponsored groups. When possible, your OSINT should explore the types and identities of known attackers who are likely to target users and usages of the technology covered by your report.

The basic question that must be answered in your OSINT report is: **what are the cybersecurity implications (good or bad) of a specific emerging application of technology**?

For this assignment, your role is that of a threat intelligence research intern working for a threat intelligence provider (private company). Your audience for this report will be subscribers to a cybersecurity threat intelligence reporting service provided by your employer. These subscribers are primarily senior managers and executives in businesses and government organizations.

The high-level visibility for your deliverable means that, in addition to easily accessed web sources and social media, your research must also include research-based journal articles, papers published in conference proceedings, and doctoral dissertations. Threat research and intelligence reports published by mainstream companies, e.g. Verizon, Forrester, Deloitte, etc., should also be considered for use as primary sources for your OSINT report. See step #3 under *Conduct Your OSINT Research* (below) for additional information about how many sources are required and what types of sources are allowed.

The following information needs, previously identified by your company’s threat researchers, must be met by the deliverable for this assignment.

1. Identification and description (characteristics) of the technology,
2. Potential or known uses of the technology to support or improve business operations of companies and government agencies; this includes development of products which incorporate the technology and potential or known uses of the technology to support or improve cybersecurity, i.e.
	1. uses of the technology to reduce or manage risk
	2. uses of the technology to increase resistance to threats/attacks
	3. uses of the technology to decrease vulnerabilities in an existing technology application
3. potential or known uses or exploitation of the technology by attackers, criminals, terrorists, etc. to accomplish their goals.

# Instructions

Format your deliverable as a research report. Your report should include the following sections:

1. Title page with author and date
2. Table of Contents (also Table of Figures if graphics are used)
3. Executive Summary
4. Introduction
5. Technology Description and Usage Analysis
6. Threat Analysis
7. Summary and Conclusions
8. Reference List

## Choose an Emerging Application of Technology

To begin, choose an emerging application of technology. Applications of technology that are currently in the *emerging* stages include:

* 5G/6G Telecommunications Technologies & Implementations (Networks)
* Artificial Intelligence
* Autonomous Vehicles (ground, sea, or air)
* Blockchain Technology
* Data Science
* Deep Space Communication Networks
* Graphene
* Implantable Medical Devices (including brain, prosthetics, medication delivery, cardiac support, etc.)
* Infrastructure for Smart Cities (surveillance, monitoring, traffic control, utilities, etc.)
* Internet of Things (especially Operational Technology)
* Internet of Things Devices in Smart Homes / Smart Buildings
* Machine Learning
* Nano machines
* Neuromorphic computer chips
* Physical Unclonable Functions (PUFs) (devices & electrical circuits)
* Precision Agriculture (integrated systems using satellite imagery, GPS, Sensors, Robots)
* Robot inspectors for physical infrastructures (buildings, roads, railways, pipelines, etc.)
* Wearable Sensors for Hazardous Materials Detection (e.g. CBRNE): Emergency Services Sector

You are encouraged to look for and investigate additional appropriate technologies before deciding upon your technology choice for this assignment.

If you decide to research a technology that is not on the suggested technologies list (see above) or included in the course readings, you must first request and receive your instructor’s permission. Your instructor may require that you do preliminary library searches for research papers and technical papers to prove that you can find a sufficient number of resources to complete the assignment.

## Conduct Your OSINT Research & Information Acquisition

**Step 1.** Review this UMGC library guide to help you evaluate sources for your OSINT Research: <https://sites.umgc.edu/library/libhow/credibility.cfm>

**Step 2.** Brainstorm keywords that you can use to help find Internet sources of information about your chosen technology. You can also search for and review articles and postings in well known cybersecurity industry blogs, news articles, and social media accounts. See <https://agio.com/newsroom/the-top-10-cybersecurity-blogs-for-2021/> and <https://libguides.umgc.edu/cybersecurity> for lists of resources. You must find and use at least five different sources in this category (Internet sources).

**Step 3.** Use your initial set of sources to develop additional keyword lists to use in searching the UMGC library databases for professional journal articles, papers, and other scholarly publications (“sources’) which discuss your chosen emerging application of technology. You must find and report on five (5) or more Open Sources which you obtained from Internet web pages, social media, etc. You must also find and report on an additional five or more Open Sources which you obtained from databases which index professional and academic papers (see <https://sites.umgc.edu/library/libhow/scholarlyjournals.cfm> if you are not sure what this means). The following UMGC library and/or freely available Internet databases are known to have suitable professional and/or research-based articles which meet the “databases” as source requirement:

* ACM Digital Library <http://ezproxy.umgc.edu/login?url=http://www.acm.org/dl>
* Dissertations & Theses (Pro Quest) <http://ezproxy.umgc.edu/login?url=http://search.proquest.com/pqdtft/advanced?accountid=14580>
* IEEE Computer Society Digital Library <https://www-computer-org.ezproxy.umgc.edu/csdl/home>
* Research Gate <https://www.researchgate.net/> (required free account to access papers)
* ARVIX <https://arxiv.org/>
* Science Direct <http://ezproxy.umgc.edu/login?url=http://www.sciencedirect.com/science/search>

Since the point of this OSINT search is to find information about *emerging* applications of technology, your sources must have a publication date of 2017 or later (2017, 2018, 2019, 2020, 2021). For papers indexed in Science Direct, you may also use papers that are marked “In Press.”

When you have finished your research for this assignment**, you should have 15 or more well chosen, high quality, authoritative resources which you will use to meet the content requirements of this project. At least 5 of those resources must be from the professional literature**, i.e. peer-reviewed journal articles, government or corporate documents or reports, trade publications, etc. See <https://sites.umgc.edu/library/libhow/credibility.cfm> and <https://sites.umgc.edu/library/libhow/scholarlyjournals.cfm> for additional information about evaluating sources.

5. Decide if you need to add images or not (including pictures, charts, graphics, etc.). If you do include images, you must make sure that each such item has a caption and that the caption includes the in-text citation for the source of the image (add the source to your list of references). The image must be readable (in focus, not blurry) and of an appropriate size. Any image or picture used MUST significantly add to the content and help the reader to understand your analysis. Do not add gratuitous imagery (no “eye candy” or decorative images). Do not add images just to increase your page count!

Note: if you have captioned items, you must include a Table of Figures after your Table of Contents.

## Putting It All Together

1. Consult the grading rubric for specific content and formatting requirements for this assignment.
2. Your 8 to 12 page OSINT report should be professional in appearance with consistent use of fonts, font sizes, margins, etc. You should use headings and page breaks to organize your paper. Title page, table of contents, and reference list do not count against the page count. Remember that your audience will benefit more from a clear, concise, and accurate presentation of information. Adding extra content just to artificially meet a page count (or exceeding the recommended length by adding filler) will not improve your grade.
3. Your paper should use standard terms and definitions for cybersecurity.
4. The CSIA program recommends that you follow standard APA formatting since this will give you a document that meets the “professional appearance” requirements. APA formatting guidelines and examples are found under Course Resources. An APA template file (MS Word format) has also been provided for your use. CSIA\_Paper\_Template(TOC+TOF,2021).docx.  This file has the style gallery set up so that you can use the built-in features of MS Word to generate a Table of Contents and, if needed, a Table of Figures.
5. Your submitted file must include a separate cover page at the beginning which provides the assignment title, your name, and the due date. Your reference list must begin with a new (separate) page at the end of your file.
6. You are expected to write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.
7. You are expected to credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must follow a consistent citation style (APA, MLA, etc.).
8. See the “Examples” section (below) for information about how to create a Table of Contents and Table of Figures. The built-in help for MS Word will also walk you through creating these content elements for your OSINT report.

# Examples

Table of Contents

[Objective 1](#_Toc74229197)

[Overview 1](#_Toc74229198)

[Instructions 2](#_Toc74229199)

[Choose an Emerging Application of Technology 2](#_Toc74229200)

[Conduct Your OSINT Research & Information Acquisition 3](#_Toc74229201)

[Putting It All Together 4](#_Toc74229202)

[Examples 5](#_Toc74229203)

[References 7](#_Toc74229204)

The Table of Contents (TOC) above was generated using MS Word’s References > Table of Contents feature (see Figure 1). You must use the headings styles from the Style Gallery in order to have the TOC generated for you.

The Table of Figures (References > Insert Table of Figures) requires that you use the Style Gallery’s “caption” style. An example of the Style Gallery window is shown in Figure 2.

When using Heading or Caption Styles in the Style Gallery, you can (should) change them to Black Font, 11 or 12 point, and add space before and after. Use the help feature in MS Word if you do not already know how to make these changes.



Figure 1. Reference Tab in MS Word (Microsoft, 2021)



Figure 2. Style Gallery in MS Word (Microsoft, 2021).

# References

Microsoft. (2021). Microsoft Word (Office 365). Redmond, WA: Author.