Artificial Intelligence Will Revolutionize the Way Intelligence is Analyzed
By Amanda Custer

It is no secret that artificial intelligence will drastically change the national security and defense sector over the coming years. Progress is being made at great speed that allows programs to process and exploit massive quantities of data and glean information from them. Analysts will now be able to fully utilize all sources and quantities of information available. The intelligence production cycle of tasking, collecting, processing, exploiting, and disseminating intelligence will adapt and shift to meet the new pace that artificial intelligence will allow. Artificial intelligence is and will be a catalyst in collecting, processing, and exploiting intelligence. While human skill and oversight will still be needed, smart programs will streamline jobs which were previously constrained by the need for labor by human analysts in tasks involving vast quantities of data. Artificial intelligence will, therefore, make intelligence analysis highly efficient and much more effective as machine learning, computer vision, and algorithms advance.

Artificial intelligence will have an impact on each discipline of intelligence. Though the specific impact will vary across the five general types of intelligence collection, all five disciplines will be streamlined to yield greater actionable intelligence. The five general types of intelligence collection are defined as open source intelligence (OSINT), signals intelligence (SIGINT), geospatial intelligence and imagery intelligence (GEOINT/IMINT), measurement and signature intelligence (MASINT), and human intelligence (HUMINT). To see the trajectory artificial intelligence will take within the intelligence process requires examining the implications of current technological advances in the field.

Open source intelligence, or OSINT, which accounts for roughly 75% of all intelligence, will be drastically more useful and efficiently exploited with the implementation of artificial intelligence programs. The collection of publicly available information is inherently a time-consuming job given the scope and
volume of sources being produced each day in our modern world. Artificial intelligence programs that accurately flag content for processing and exploitation by human analysts will yield actionable intelligence in an efficient and timely manner. Given the volume of open source intelligence which is generated daily by the exponential nature of data on the Internet, artificial intelligence will be poised to alleviate the challenge which this poses to analysts. Open source intelligence will also foster public innovation through the development of open source technology that will grow the capabilities of the intelligence community.

Open source technology’s role in creating solutions through the development of artificial intelligence tools will spur progress and accessibility for those seeking to utilize the advantages of artificial intelligence. The power of developments for artificial intelligence in open source forums can be seen in cases such as Lobe, a new startup. Lobe launched an app which offers users the ability to create deep learning algorithms without having to write a single line of code. Using machine vision, Lobe allows users to build object recognition through their own webcam, collecting the ‘data’ by taking photos, labeling that data to identify and categorize the objects, and then having a neural network learn from the collected data and labels. Users can export their final model to varying platforms including Google’s TensorFlow, an open source AI platform. Their services are completely free to users. While Lobe is not very sophisticated and still in the Beta phase, this tool would eliminate, or to some degree mitigate, the need for specialized skills to write a program for object detection. Though Lobe lacks the sophistication of its manually-coded counterparts, it possesses the potential to make the desired outcomes of object recognition for example, easier and cheaper to acquire by those with access to the internet.

Signals intelligence (SIGINT), which is comprised of communication intelligence (COMINT) and electronic intelligence (ELINT), will benefit from AI’s machine learning by accelerating the detection of patterns and processing of the intelligence. Signals intelligence is the underlying component of cyber warfare. There is increasing concern over cyber warfare as the shift in daily affairs, commerce, and security go digital and leave people and nations vulnerable to exploitation of their data and exposure of physical system structures linked to the digital world. Artificial intelligence stands to increase both sides of cyber warfare, the offense and the defense. Robust cyber programs such as Stuxnet, a program developed which is widely known for its interference with Iran’s nuclear program, stand to change the way the cyber world affects physical security. By the same token, these cyber programs and models provide artificial intelligence with tools and strategies that can be tested in the physical world.

Artificial intelligence’s role as a platform for learning and testing new strategies in the physical world can be seen in innovations such as the United Kingdom’s Ministry of Defense report highlighting artificial intelligence using war video games to learn strategy and tactical reasoning in cyber warfare. This example of how artificial intelligence stands to enhance the capabilities of SIGINT technology brings into question the increasing concern over the chances of rogue states and terrorists mounting advanced persistent threat attacks. AI perpetrated attacks require less skill, in comparison to the sophistication of Stuxnet for example, and AI algorithms are becoming more accessible through machine learning. However, in this way, the intelligence community stands to gain greater strategic capital.

**Development of computer algorithms for object detection, alerts, and classification provides DoD with the ability to analyze significant quantities of drone footage and images by flagging content with pertinent criteria for human review.**

Geospatial intelligence and imagery intelligence (GEOINT/IMINT) collect intelligence through electro-optical, infrared, and radar imagery collection. The development of technologies in artificial intelligence such as object detection and computer vision would serve to greatly reduce the high volume of content which human analysts must examine. The creation of computer programs that would allow the U.S. intelligence community to fully utilize all the collected images and video on any
A given day increases the chances of gaining actionable intelligence that could provide warning of other top US tech firms such as Microsoft, brings to the project their open source machine learning TensorFlow AI platform.

The development of a similar AI machine learning project by the Pentagon is working to detect potential nuclear missile strikes by creating a system that could process huge amounts of data such as satellite images to search for characteristics of a missile launch. This program, similar to Project Maven, would allow analysts to efficiently analyze the large quantity of data collected each day and create actionable intelligence. Therefore, more time would be allowed to make a decision should a critical situation arise such as the launching of a nuclear missile. The graphic demonstrates the system's use and how these technologies will use available intelligence.

Measurement and signature intelligence, or MASINT, is defined as intelligence which "determines, locates,
tracks, identifies, and/or describes the specific characteristics of fixed and dynamic target objects and sources.” This includes advanced processing and exploitation of data derived from IMINT and SIGINT collection. With MASINT being a multifaceted intelligence type, the posterior advances in artificial intelligence stand to make an impact in MASINT’s processing and exploitation. MASINT stands to gain efficiency and some degree of automation through artificial intelligence through programs such as Project Maven with image and video recognition software providing automated tools for identifying objects and characteristics of those objects. Using the footage gleaned from UAS and mid-altitude FMV, artificial intelligence will greatly reduce the manpower needed to identify actionable information and characteristics.

Human intelligence (HUMINT) is a discipline of intelligence that will be the least directly transformed by the integration of artificial intelligence into the analysis of intelligence, but several developments of AI could play helpful roles in targeting and surveillance. Innovations in technologies such as facial recognition, and other tools that allow surveillance to identify people accurately and quickly, will enhance the targeting and assessment of human sources. Many of the developments in this realm have been developed for the private sector with applicability in more customary fashions of everyday life but these developments have applications in the surveillance and targeting arena.

Professor Dina Katabi and her research team from MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL) has developed a technology which will greatly transform how surveillance can be conducted. The team has made significant progress in project “RF-Pose” which uses artificial intelligence to “teach wireless devices to sense people’s postures and movement, even from the other side of a wall.” The technology uses AI to teach wireless devices to track a person’s movement through walls by using a neural network that analyzes radio signals bouncing off human bodies to trace figures and movements. These radio waves are 1,000 times milder than standard Wi-Fi and can track human movement with detail. RF-Pose is able to estimate a person’s posture and movements without cameras, using only the wireless reflections that bounce off people’s bodies, and has been able to accurately identify a person 83 percent of the time out of a line-up of 100 individuals. The technology primarily focuses on the implications for the use in healthcare monitoring of elders and patients with Parkinson’s disease. This development in technology poses a new level of surveillance abilities. The integration of this technology into surveillance technology can provide more detailed information about persons on the ground than previously available through say that of infrared imaging employed in IMINT.

The market research agency Kantar Millward Brown is using technology developed by US firm Affectiva to deploy an algorithm that can detect a person’s mood. This advancement in computer vision and artificial intelligence is extremely useful in the commercial sector for targeted marketing and product placement. However this “emotion detection” carries with it surveillance and security implications as well. The UK firm WeSee has already cashed in on this use of the technology, claiming that its AI technology can identify suspicious behavior through the reading of subtle facial clues. The accuracy of this technology is still far from being a reliable source on its own, but as the machine learning and neural networks improve so will the accuracy. This is already
evident in the realm of commerce and security as the world moves to use facial recognition to unlock smartphones, identify people at borders, authenticate banking transactions, and spot criminals.

Amazon’s launch of Echo Look in the US could popularize the use of computer vision across American households via Alexa. This broader use by the public of computer vision will provide more data and development opportunities for the creation of computer vision systems across the private sector. The advances being made in computer vision by Amazon will be deployed by their personal assistant devices to act as a retail marketing and advertising device and will have computer vision surveillance applicability.13 Echo Look’s primary function is to provide tailored fashion advice to customers with the goal of users making their purchases through Amazon’s clothing and fashion sales. Integrating computer vision to deploy object recognition and make judgments on colors, sizes, and styles have applicability in the surveillance and security sector for assessing human targets.

The development of a Virtual Positioning System (VPS) requires the use of computer vision to analyze in real time the location and surroundings of a device and can determine the location of an individual or object within the context of the environment.14 This development will allow persons with access to the data of a device using VPS to know the precise location of the device holder within their environment, which will greatly enhance the level of detail in surveillance. Unlike traditional GPS systems, the VPS’s ability to tell the orientation of an object or individual within their surrounding environment provides enhanced information in comparison to global positioning and imagery alone. VPS was originally intended to determine the precise orientation and location of a user’s phone for enhanced virtual reality applications. However, having an accurate three-dimensional location is also a critical tool for comprehensive intelligence gathering. This would give intelligence professionals a much more detailed image of a human target’s movement, environment, and location.

In conclusion, studying artificial intelligence and the advances in the field is a never-ending task in which one is always behind. Combining existing AI technologies yields new capabilities which once deployed give rise to the need for additional technologies. Once those technologies are developed and deployed, the cycle repeats itself. With each iteration, artificial intelligence becomes more disrupting, creating revolutions in the way intelligence is analyzed.

Innovations of the hardware in technology also continue to evolve which will greatly change how software and artificial intelligence can be deployed. Though these innovations are still only potential leaps forward for the future of artificial intelligence packing more of a punch into less space, they stand to further expand how and where the technology can be employed. IBM has recently found that the construction of neural networks directly onto silicon, rather than conventional computer chips which the software normally runs on, would be “100 times more efficient” for both computing and energy.15 While the chips being tested are neither complete nor compact yet, the implications of having faster and more efficient neural networks stand to revolutionize where and how AI can be used for both commercial and defense purposes.16 Advances in this technology would make the computing power of artificial intelligence easier to incorporate across the five different types of intelligence by reducing its physical presence.

However, as artificial intelligence improves the ability to process and exploit available intelligence, human analysts will still be necessary and critical for the process. Artificial intelligence will greatly reduce the labor and time needed to exploit the tremendous quantity of existing data from which intelligence analysts glean relevant information. The advances in technology will make analysts more efficient at their jobs and allow the intelligence community to better utilize all available sources and tools at their disposal. Artificial intelligence will, therefore, improve the efficiency and accuracy of intelligence gathered across all forms.
Amanda Custer is a Senior at Dickinson College pursuing a double major: a B.A. in International Studies with a focus on Security Studies and a B.A. in Spanish. Amanda has developed her professional experience in the field through two completed undergraduate research internships at the Peacekeeping and Stability Operations Institute at the US Army War College. Both of her research findings were published by PKSOI in their Peacekeeping and Stability Journal. Amanda spent this past summer doing research at the Institute of World Politics, where she researched the implications of artificial intelligence in the intelligence community.

1. Lowenthal, Mark M. Intelligence: From Secrets to Policy. Sage, 2015
3. Ibid.
12. Ibid.
16. Ibid.