Robotics and The Automation of National Defense

Benjamin S. Benoit

University of Louisville

Robotics and The Automation of National Defense

Technology is ever evolving prospect, with the arrival of electronic computation, mankind has witnessed what appears to be an area of scientific innovation without limits, each evolution in technology hastens future innovations. An example would be self-improving artificial intelligence, that essentially utilizes an underlying infrastructure and mathematical foundation to further improve itself. This is done often with efficiency that makes even the most intelligent of humans seemingly obsolete. It is a frightening prospect. So much of our society is based up notions of labor, and self-earned merit. Historically robotics and artificial intelligence have been replacing unspecialized labor, in other words manufacturing. This has had devastating impacts to the middle-class economy, while elevating and improving the economic prosperity of those who control the intellectual property of said robotics and AI. Robotics has literally altered the economic ecosystem of those without higher education (predominantly), but slowly there has been a trend towards replacing specialized labor. This paper will examine AI and robotics on a macro level as it applies to the military and policing. Given the implications of replacing a police officer with a robot, or an infantry person with a robot, this paper will examine the possible complications and benefits of a robotics interacting with and policing human beings. It will also cover the infrastructural demands of creating a robotics armed forces and police state. This paper will also cover briefly the ethical implications of establishing such technology.

The underlying required infrastructure for remotely controlled robotics has been greatly limited historically by our telecommunications industry. The underlying networks that bring communications of data that interconnect us, has not evolved to the point that mobilized robotics unit could be efficiently and effectively controlled remotely. To understand the complications of this, one must examine and breakdown the individual inputs and outputs that would be required to effectively control and utilize a machine capable of killing a living person. A prime example of this would be with drones, although measurably effective in eliminating armed combatants and terrorist, they are not perfect. There have been countless incidences of civilians being horribly maimed or murdered unintentionally by such technology. The implications of having a machine that is essentially collecting external stimuli processing this and making decision of life or death are daunting. A simple miscalculation or miscommunication could result in numerous deaths. Imagine what would happen if a robot armed with guns suffered from a serious glitch that caused it to deem a crowd of people as enemy combatants, or dangerous criminals. Countless may die before this robot could be stopped.

A networked robotic system is classified as a group of robotic instruments that are connected through a wired or wireless communications network. Their applications are classified within two distinctions, multi-robot systems or teleoperated robots. Teleoperated robots refer to a robot that is operated by a human at a distance. Examples of this would be planetary rovers or robots used in remote medical surgery. A multi-robot system is a system of robots that are networked together and cooperatively complete tasks by sharing data through a communications network. An example of this would be micro satellites collecting data cooperatively. There are many limitations for networked robots, due to computation occurring within the robot, the limitations of the network limit its efficiency. Cloud robotics aim to resolve these issues. The amount of information that is accessible to a robot is fettered by its individual computational power. Cloud-enabled networked robotics utilizes new cloud computing technologies to improve networked robotics.  
 The systems architecture of cloud robots is organized into two tiers of communication. The first is machine-to-machine level, the second would be machine-to-cloud level. On the M2M level a group of robots would communicate via a wireless link to effectively form what is known as a “collaborative computing fabric” This offers a myriad of benefits; computing capability of individual robots is pooled to form a virtualized ad-hoc cloud. Information can then be shared for decision making. Next, on the machine to cloud level, the cloud collects pooled data of computation and storage resources, which can be accessed in real time remotely by the robots. This allows for robots to share workloads of difficult computational tasks that it couldn’t resolve on it own due to the limitations of its computational power. Thus, an offsite supercomputer could be utilized to quickly solve these computational needs, and communicate this back to the cloud, which would then communicate this data back to the robots. For short range Wi-Fi and Bluetooth could be used, for long range radio frequency, microwave technologies could be used. But, with the innovation of 5g networks long-distance communications amongst robots could be drastically improved.

Advanced 5g infrastructure is defined as the ubiquitous ultrabroadband network, this would be the fifth generation of network communications for mobile devices. This network system is expected to be the backbone of our telecommunications industry by the year 2020. The 5G operating system will allow servers in a centralized data center to act as administrator, controlling data and security and allowing functions of connected devices. What this means in terms of robotics is a reduction to 1 millisecond latency for remotely controlled robots, and basically there would be no communicative dead zones, an issue that previously would limit the utilization of robotics capabilities. About 40 GHz could be allocated for massive machine objects and cyber-physical systems (robots, self-driving cars, drones). This fundamentally alters the previous client-server model of telecommunications to a neural bearer model. That is devices are no longer limited to the end-to-end connectivity because of 5G’s open and flexible infrastructure. 5G will allow authorized devices access through software-defined and virtualized architecture. In order to accomplish this, radio access nodes will have to be redesigned. Fiber access for fixed networks would have to be underlying network that supports the infrastructure of the 5g network. Additionally, large quantities of data will be generated as a result of these improvements. Creating a need for improved storage capabilities, and improved protocols for access stratum and NAS. Protocols would provide security for said networks. Multiple-input, multiple output techniques will be used to improve coverage and reduce interference. These MIMO’s would consist of large planar antenna arrays. These MIMO’s would have three levels of controllers. First would be device controllers, which are located locally within the device allowing access to the 5G network. Second, edge controllers, which would perform radio resource management and adaptive layer functions (controlling packets). Finally, orchestration controller, which enables coordination of cloud computing resources and distributed networking. The three levels of controllers allow interfaces from the outer world to a myriad of services or networks.

Latency plays a huge role in the utilization of robotics. Soldani and Manzalini present the three levels of controllers interacting with three levels of programmed reactive intelligence as a solution. The first would be automatic reactions, or predefined actions with localized specific context, this would require a match action within the programming of the robot. In other words, a true or false condition, prior to an action. The second is autonomic reaction, that is action created via data analytics systems and methods, which occur as a result of elaborating on large amount of localized data which is controlled by deep learning artificial intelligence capabilities. These intelligent tasks would be performed at data centers and then communicated to the remotely controlled robot. Third orchestrated behavior, which are actions based on data analytics systems and methods after elaboration on large amounts of data from different localized contexts. These capabilities would reside within a cloud, not on the robots localized infrastructure.

There are three proposed computing models for cloud robots. The first of which is a peer-based model, that is each robot is a virtual machine in a ubiquitous cloud and considered a computing unit. A task can be divided into smaller modules that are executed by a subset of nodes over a computing mesh. The second is a proxy-based model, in which a group of networked robots are controlled by a group leader, communicating with a proxy virtual machine in the cloud infrastructure. Communications and interactions are bridged by the robotics network and the cloud. The last model is a clone-based model, where each robot has a corresponding level clone in the cloud. A task can be completed by the robot or its clone. These clones establish a peer-to-peer network over a machine to machine network.

The security of such a network of robots presents considerable obstacles. The virtual machine environment needs to be secure. A saboteur could infiltrate and corrupt this virtual environment without the robots being aware. This could have devastating implications in a military or policing situation. In such application robots must identify a trustworthy virtual machine infrastructure to avoid connecting to ill-intended ones. Hu presents a resolution via three measures of trust approaches. First trust establishment, that is the user performs some pre-use action to check a virtual machine’s host environment. Second trust measurement, that is some components that do not belong to the cloud platform monitor the virtual machine and report trust measurements to a third party. Lastly reputation-based trust, that is the user verifies the virtual machine infrastructure by the service providers identity and then relies on external legal considerations to allow trust. With the combination of these safety measure, one could properly prevent hackers, or even foreign governments from infiltrating and causing great harm and damage to civilians being monitored by police or military robots. A robot needs trust to delegate tasks on a public cloud. Confidential data may be stored in the cloud. Requiring strong integrity and confidentiality protection when utilizing application data.

The image of a “killer robot”, still largely belongs to the world of science fiction. Although existing prototypes like the PROWLER and the BRAVE 3000, are not autonomous, these weapons demonstrate that true artificial intelligence is not yet needed to create robotics war machine. The PROWLER is a terrestrial armed vehicle, equipped with machine vision, that is it can analyze contents within a video frame. This allows it to distinguish allies from combatants. The Russian FEDOR is Russia’s newest robot capable of shooting two guns accurately at targets. Though the underlying technology is relatively unknown, Russia is set with the aim of developing a robotic army, one must find such developments to be alarming. The US Navy X-47B program developed an unmanned combat air vehicle which by 2015 had conducted the world’s first fully autonomous aerial refueling. The US AFRL project named “ALPHA” developed a flight simulator in which an AI was put against experienced combat pilots, and won in a variety of air-to-air combat scenarios. The Army has established a variation of manned and unmanned vehicle operation named MUM-T. Establishing tactic and techniques and procedures by outfitting its aviation combat brigades with manned 64D/E apache helicopters and Textron Systems RQ-7B Shadow Tactical Unmanned Aircraft Systems. The expectation is to enhance surveillance of the surrounding environment and enhance decision making.

The UN has voted to begin formal discussions on the use of autonomous weapons. An open letter to the UN signed by 116 artificial intelligence experts called for a ban on such weaponry stating: “Once developed, lethal autonomous weapons will permit armed conflict to be fought at a scale greater than ever, and at timescales faster than humans can comprehend. These can be weapons of terror, weapons that despots and terrorists use against innocent populations, and weapons hacked to behave in undesirable ways.”

In conclusion the future of robotics and artificial intelligence is unquestionably frightening, especially when it comes to military applications and policing of individual citizens. The possibility of great harm to our economy, by displacing workers such as police officers, military members as well as a myriad of other non-military-based professions such as truck drivers is a reality our society must one day face. The dangers of autonomous robots and other types of equipment (with the capability of killing humans) could be the cause of what many would call an “apocalypse” or the literal end of human race. Thus, this matter calls for caution amongst our scientific community. Unbridled scientific innovation could cause death and chaos beyond our current comprehension. So precarious measures should be avoided. Our society must not just develop these war machines with merely a hope that things won’t go wrong. Scientist must take our obliteration in to account with every step toward developing robotics and autonomous weaponry. Though it is some time off before we fully develop the underlying 5G networks needed to have functioning robots that scale outside the realm of manufacturing, the day when AI and robotics take over driving cars, completing military operations, policing society and other dangerous jobs once completed by humans is not far. What matters is that our world approaches this with empathy, and consideration towards human civilization, and the maintenance of civil society. Such power in the hands of wicked person could be catastrophic and instead of technology propelling us towards a great future, it would be propelling us to a great end.

References

Last Name, F. M. (Year). Article Title. *Journal Title*, Pages From - To.

Last Name, F. M. (Year). *Book Title.* City Name: Publisher Name.