Evolution Continues With Quantum Biology and Artificial Intelligence

Robert Skopec

Dubnik, Slovakia, Researcher-analyst

ABSTRACT

Artificial Intelligence (AI) research has a lot to learn from nature. My work links biology with computation and AI every day, but recently the rest of the world was reminded of the connection: The 2018 Nobel Prize in Chemistry went to Frances Arnold together with George Smith and Gregory Winter for developing major breakthroughs that are collectively called “directed evolution.” One of its uses is to improve protein functions, making them better catalysts in biofuel production. Another use is entirely outside chemistry – outside even the traditional life sciences. It’s about my main innovation that Evolution continues with Artificial Intelligence and at the field of Quantum Biology, through the Economics, until the field of Military Self-Defense.

Keywords
Directed Evolution, Artificial Intelligence, Quantum Biology, protein functions, Quantum Entanglement Entropy, algorithms, Computational Evolution, the neocortex, mutations, computerized intelligent systems.

Conflict of Interests Disclosure
Author declares no conflict of interests.
Introduction
That might sound surprising, but many research findings have very broad implications. It’s part of why just about every scientist wonders and hopes not only that maybe they would be selected for a Nobel Prize, but, far more likely, that the winner might be someone they know or have worked with. In the collaborative academic world, this isn’t terribly uncommon: In 2002, I was studying under a scholar who had studied under one of the three co-winners of that year’s Nobel Prize in Physiology or Medicine. This year, it happened again – one of the winners has written a couple of papers with a scholar I have collaborated with. (Hintze, 2018)

Evolution of Quantum Biology and Artificial Intelligence
Beyond satisfying my own vanity, the award reminds me how useful biological concepts are for engineering problems. The best-known example is probably the invention of Velcro hook-and-loop fasteners, inspired by burrs that stuck to a man’s pants while he was walking outdoors. In the Nobel laureates’ work, the natural principle at work is evolution – which is also the approach I use to develop artificial intelligence. My research is based on the idea that evolution led to general intelligence in biological life forms, so that same process could also be used to develop computerized intelligent systems. (Skopec I., 2017, Skopec II., 2018)

When designing AI systems that control virtual cars, for example, you might want safer cars that know how to avoid a wide range of obstacles – other cars, trees, cyclists and guardrails. My approach would be to evaluate the safety performance of several AI systems. The ones that drive most safely are allowed to reproduce – by being copied into a new generation.

Yet just as nature does not make identical copies of parents, genetic algorithms in computational evolution let mutations and recombinations create variations in the offspring. Selecting and reproducing the safest drivers in each new generation finds and propagates mutations that improve performance. Over many generations, AI systems get better through the same method nature improves upon itself – and the same way the Nobel laureates made better proteins. (Paulus and Frank, 2006)

In the effort to understand human intelligence, many researchers are working to reverse-engineer the brain, figuring out how it works at all levels. Complex gene networks control the neurons that form the layers of the neocortex that are sitting on top of a highway of connections. These interconnections support communications between the different cortical regions that make up most of our cognitive functions. All of this is integrated into the phenomenon of consciousness. (Gold and Shadlen, 2007, Hsu et al., 2009)

Deep learning and neural networks are computer-based approaches that attempt to recreate how the brain works – but even they can only achieve the equivalent activity of a clump of brain cells smaller than a sugar cube. There remains an enormous amount to learn about the brain – and that’s before trying to write the intensely complicated software that can emulate all those biological interactions. Capitalizing on Evolution can make systems that seem lifelike and are inherently as open-ended and innovative as natural evolution is. It is also the key methodology used in genetic algorithms and genetic programming. The Nobel Prize committee’s recognition highlights a technology that has evolution at its core. That indirectly justifies my own research approach and the idea that evolution in action is a critical research topic with vast potential.

Materials and Methods: Explaining public-key cryptography
As I’m working on a product that will make heavy use of encryption, I’ve found myself trying to explain public-key cryptography to friends more than once lately. To my surprise,
anything related I’ve come across online makes it look more complicated than it should. But it’s not.
First of all, let’s see how “symmetric” cryptography works. John has a box with a lock. As usual, the lock has a key that can lock and unlock the box. So, if John wants to protect something, he puts it in the box and locks it. Obviously, only he or someone else with a copy of his key can open the box. That’s symmetric cryptography: you have one key, and you use it to encrypt (“lock”) and decrypt (“unlock”) your data.
Now let’s see how asymmetric, or “public-key” cryptography works. Anna has a box too. It’s a box with a very special lock.

Motor and Sensory Regions of the Cerebral Cortex

![Motor and Sensory Regions of the Cerebral Cortex](https://example.com/cerebral_cortex_image)

Figure 1. A map of the cerebral cortex. Bruce Blaus/wikimedia, CC BY

![Lock Diagram](https://example.com/lock_diagram)

Thanks to @leedykxhoorn for the illustration. This lock has three states: A (locked), B (unlocked) and C (locked).
And it has two separate (yes, two) keys. The first one can only turn clockwise (from A to B to C) and the second one can only turn counterclockwise (from C to B to A). Anna picks the first one of the keys and keeps it to herself. We will call this key, her “private” key-because only Anna has it.

We will call the second key, her “public” key: Anna makes a hundred copies of it, and she gives some to friends and family, she leaves a bunch on her desk at the office, she hangs a couple outside her door, etc. If someone asks her for a business card, she hands him a copy of the key too.

So. Anna has her private key that can turn from A to B to C. And everyone else has her public key that can turn from C to B to A. We can do some very interesting things with these keys.

First of all, imagine you want to send Anna a very personal document. You put the document in the box and use a copy of her public key to lock it. Remember, Anna’s public key only turns counterclockwise, so you turn it to position A. Now the box is locked. The only key that can turn from A to B is Anna’s private key, the one she’s kept for herself.

That’s it! This is what we call public key encryption: Everyone who has Anna’s public key (and it’s easy to find a copy of it, she’s been giving them away, remember?), can put documents in her box, lock it, and know that the only person who can unlock it is Anna.

There is one more interesting use of this box. Suppose Anna puts a document in it. And she uses her private key to lock the box, i.e. turn the key to position (C). Why would she do this? After all, anyone with her public key, can unlock it! Wait.

Someone delivers me this box and he says it’s from Anna. I don’t believe him, but I pick Anna’s public key from the drawer where I keep all the public keys of my friends, and try it. I turn right, nothing. I turn left and the box opens! “Hmm”, I think. “This can only mean one thing: the box was locked using Anna’s private key, the one that only she has.”

So, I’m sure that Anna, and no one else, put the documents in the box. We call this, “digital signature”. In the digital world things are much easier.

“Keys” are just numbers -big, long numbers with many digits. You can keep your private key, which is a number, in a text file or in a special app. You can put your public key, which is also a very long number, in your email signature, your website, etc. And there is no need for special boxes, you just “lock” and “unlock” files (or data) using an app and your keys.

If anyone, even you, encrypt (“lock”) something with your public key, only you can decrypt it (“unlock”) with your secret, private key. (Vryonis, 2018)

If you encrypt (“lock”) something with your private key, anyone can decrypt it (“unlock”), but this serves as a proof you encrypted it: it’s “digitally signed” by you. (By Koppas (Own work)

They can also get much more complicated: We can use our private key to sign a file and then someone else’s public key to encrypt it so that only he can read it. And one user, or an organisation, can digitally sign other users’ keys, to verify their authenticity, etc, etc. But all this actually breaks down to using the one or the other key and putting boxes into other boxes -and it’s outside the scope of this article. (Vryonis, www.vrypan.net, http://blog.vrypan.net/)

Computers capable of explaining their decisions to military commanders

The Defense Department’s cutting-edge research arm has promised to make the military’s largest investment to date in artificial intelligence (AI) systems for U.S. weaponry, committing to spend up to $2 billion over the next five years in what it depicted as a new effort to make such systems more trusted and accepted by military commanders.
The director of the Defense Advanced Research Projects Agency (DARPA) announced the spending spree on the final day of a conference in Washington celebrating its sixty-year history, including its storied role in birthing the internet.

The agency sees its primary role as pushing forward new technological solutions to military problems, and the Trump administration’s technical chieftains have strongly backed injecting artificial intelligence into more of America’s weaponry as a means of competing better with Russian and Chinese military forces.

The DARPA investment is small by Pentagon spending standards.

The DARPA investment is small by Pentagon spending standards, where the cost of buying and maintaining new F-35 warplanes is expected to exceed a trillion dollars. But it is larger than AI programs have historically been funded and roughly what the United States spent on the Manhattan Project that produced nuclear weapons in the 1940’s, although that figure would be worth about $28 billion today due to inflation.

In July defense contractor Booz Allen Hamilton received an $885 million contract to work on undisclosed artificial intelligence programs over the next five years. And Project Maven, the single largest military AI project, which is meant to improve computers’ ability to pick out objects in pictures for military use, is due to get $93 million in 2019.

Turning more military analytical work – and potentially some key decision-making – over to computers and algorithms installed in weapons capable of acting violently against humans is controversial.

Google had been leading the Project Maven project for the department, but after an organized protest by Google employees who didn’t want to work on software that could help pick out targets for the military to kill, the company said in June it would discontinue its work after its current contract expires.

While Maven and other AI initiatives have helped Pentagon weapons systems become better at recognizing targets and doing things like flying drones more effectively, fielding computer-driven systems that take lethal action on their own hasn’t been approved to date.

A Pentagon strategy document released in August says advances in technology will soon make such weapons possible. “DoD does not currently have an autonomous weapon system that can search for, identify, track, select, and engage targets independent of a human operator’s input,” said the report, which was signed by top Pentagon acquisition and research officials Kevin Fahey and Mary Miller.

But “technologies underpinning unmanned systems would make it possible to develop and deploy autonomous systems that could independently select and attack targets with lethal force,” the report predicted.

while AI systems are technically capable of choosing targets and firing weapons, commanders have been hesitant about surrendering control.

The report noted that while AI systems are already technically capable of choosing targets and firing weapons, commanders have been hesitant about surrendering control to weapons platforms partly because of a lack of confidence in machine reasoning, especially on the battlefield where variables could emerge that a machine and its designers haven’t previously encountered. (Ramachandran and Hubbard, 2001)

Right now, for example, if a soldier asks an AI system like a target identification platform to explain its selection, it can only provide the confidence estimate for its decision, DARPA’s director Steven Walker told reporters after a speech announcing the new investment – an estimate often given in percentage terms, as in the fractional likelihood that an object the system has singled out is actually what the operator was looking for.
“What we’re trying to do with explainable AI is have the machine tell the human ‘here’s the answer, and here’s why I think this is the right answer’ and explain to the human being how it got to that answer,” Walker said.

DARPA officials have been opaque about exactly how its newly-financed research will result in computers being able to explain key decisions to humans on the battlefield (Darimont et al., 2015), amidst all the clamor and urgency of a conflict, but the officials said that being able to do so is critical to AI’s future in the military.

Human decision-making and rationality depend on a lot more than just following rules.

Vaulting over that hurdle, by explaining AI reasoning to operators in real time, could be a major challenge. Human decision-making and rationality depend on a lot more than just following rules, which machines are good at. It takes years for humans to build a moral compass and commonsense thinking abilities, characteristics that technologists are still struggling to design into digital machines.

“We probably need some gigantic Manhattan Project to create an AI system that has the competence of a three year old,” Ron Brachman, who spent three years managing DARPA’s AI programs ending in 2005, said earlier during the DARPA conference. “We’ve had expert systems in the past, we’ve had very robust robotic systems to a degree, we know how to recognize images in giant databases of photographs, but the aggregate, including what people have called commonsense from time to time, it’s still quite elusive in the field.” (University of California-Berkeley, 2018)

Michael Horowitz, who worked on artificial intelligence issues for Pentagon as a fellow in the Office of the Secretary of Defense in 2013 and is now a professor at the University of Pennsylvania, explained in an interview that “there’s a lot of concern about AI safety – [about] algorithms that are unable to adapt to complex reality and thus malfunction in unpredictable ways. It’s one thing if what you’re talking about is a Google search, but it’s another thing if what you’re talking about is a weapons system.”

Horowitz added that if AI systems could prove they were using common sense, "it would make it more likely that senior leaders and end users would want to use them."

An expansion of AI’s use by the military was endorsed by the Defense Science Board in 2016, which noted that machines can act more swiftly than humans in military conflicts. But with those quick decisions, it added, come doubts from those who have to rely on the machines on the battlefield. (Masterson, 2018)

“While commanders understand they could benefit from better, organized, more current, and more accurate information enabled by application of autonomy to warfighting, they also voice significant concerns,” the report said.

DARPA isn’t the only Pentagon unit sponsoring AI research. The Trump administration is now in the process of creating a new Joint Artificial Intelligence Center in that building to help coordinate all the AI-related programs across the Defense Department.

But DARPA’s planned investment stands out for its scope. DARPA currently has about 25 programs focused on AI research. (Rechtsman et al., 2018),

DARPA currently has about 25 programs focused on AI research, according to the agency, but plans to funnel some of the new money through its new Artificial Intelligence Exploration Program. That program, announced in July, will give grants up to $1 million each for research into how AI systems can be taught to understand context, allowing them to more effectively operate in complex environments.

Walker said that enabling AI systems to make decisions even when distractions are all around, and to then explain those decisions to their operators will be “critically important...in a warfighting scenario.” (https://www.theverge.com/2018/9/8/17833160/
Quantum Computers Change the World

In the ancient world, they used cubits as an important data unit, but the new data unit of the future is the qubit — the quantum bits that will change computing. Quantum bits are the basic units of information in quantum computing, a new type of computer in which particles like electrons or photons can be utilize to process information with both sides (polarizations) acting as a positive or negative, alternatively or at the same time.

According to experts, quantum computers will be able to create breakthroughs in many of the most complicated data processing problems, leading to the development of new medicines, building molecular structures and doing analysis going far beyond the capabilities of today’s binary computers. (Lin et al., 2014, Kourtidis et al., 2015, Mayo Clinic, 2015)

The elements of quantum computing have been around for decades, but it’s only in the past few years that a commercial computer that could be called quantum has been built by a company called D-Wave. Announced in January 2018, the D-Wave 2000Q can solve larger problems than was previously possible, with faster performance, providing a big step toward production of applications in optimization, cybersecurity, machine learning and sampling.

IBM announced that it had gone even further — and that it expected and it would be able to commercialize quantum computing with a 50-qubit processor prototype, as well as provide online access to 20-qubit processors. That was followed by Microsoft announcement of a new quantum computing programming language and stable topological qubit technology that can be used to scale up the number of qubits.

Taking advantage of the physical spin of quantum elements, a quantum computer will be able to process simultaneously the same data in different ways (HYBRID), enabling it to make projections and analyses much more quickly and efficiently than now is possible. There are significant physical issues that must be worked out, such as the fact that quantum computers can only operate at cryogenic temperatures (at 250 times colder than deep space) — but Intel, working with Netherlands firm QuTech, is convinced that it is just a matter of time before the full power of quantum computing is unleashed.

Their quantum research has progressed to the point where partner QuTech is simulating quantum algorithm workloads, and Intel is fabricating new qubit test chips on a regular basis in their leading-edge manufacturing facilities. Intel Labs expertise in fabrication, control electronics and architecture sets us apart and will serve us well as venture into new computing paradigms, from neuromorphic to quantum computing.

The difficulty in achieving a cold enough environment for a quantum computer to operate is the main reason they are still experimental, and can only process a few qubits at a time — but the system is so powerful that even these early quantum computers are shaking up the world of data processing. On the one hand, quantum computers are going to be a boon for cybersecurity, capable of processing algorithms at a speed unapproachable by any other system. (Medrano, 2017)

By looking at problems from all directions — simultaneously (HYBRID) — a quantum computer could discover anomalies that no other system would notice, and project to thousands of scenarios where an anomaly could turn into a security risk. Like with a top-performing supercomputer programmed to play chess, a quantum-based cybersecurity system could see the moves an anomaly could make later on — and quash it on the spot.

The National security Agency, too, has sounded the alarm on the risks to cybersecurity in the quantum computing age. Quantum computing will definitely be applied anywhere where we’re using machine learning, cloud computing, data analysis. In security that
means intrusion detection, looking for patterns in the data, and more sophisticated forms of parallel (HYBRID) computing.

But the computing power that gives cyber-defenders super-tools to detect attacks can be misused as well. Scientists at MIT and the University of Innsbruck were able to build a quantum computer with just five qubits, demonstrating the ability of future quantum computers to break the RSA encryption scheme. (Hintze, 2018)

That ability to process the zeros and ones at the same time means that no formula based on a mathematical scheme is safe. The MIT/Innsbruck team is not the only one to have developed cybersecurity-breaking schemes, even on these early machines, the problem is significant enough that representatives of NIST, Toshiba, Amazon, Cisco, Microsoft, Intel and some of the top academics in the cybersecurity and mathematics worlds met in Toronto for the yearly Workshop on Quantum-Safe Cryptography last year.

The NSA’s Commercial National Security Algorithm Suite and Quantum Computing FAQ says that many experts predict a quantum computer capable of effectively breaking public key cryptography within a short time.

According to many experts, the NSA is far too conservative in its prediction, many experts believe that the timeline is more like a decade and a half, while others believe that it could happen even sooner. And given the leaps of progress that are being made on almost a daily process, a commercially viable quantum computer offering cloud services could happen even more quickly, the D-Wave 2000Q is called that because it can process 2,000 qubits. That kind of power in the hands of hackers makes possible all sorts of scams that don’t even exist yet. (Gibbons, 2018)

Forward-looking hackers could begin storing encrypted information now, awaiting the day that fast, cryptography-breaking quantum computing-based algorithms are developed. It’s certain that the threats to privacy and information security will only multiply in the coming decades. In fact, why wait? Hackers are very well-funded today, and it certainly wouldn’t be beyond their financial abilities to buy a quantum computer and begin selling encryption-busting services right now. It’s likely that not all the cryptography-breaking algorithms will work on all data, at least for now. This is a threat-in-formation – but chances are that at least some of them will, cyber-criminals could utilize the cryptography-breaking capabilities of quantum computers, and perhaps sell those services to hackers via the Dark Web. (Fryer-Biggs, 2018)

The solution lies in the development of quantum-safe cryptography, consisting of information theoretically secure schemes, hash-based cryptography, code-based cryptography and exotic-sounding technologies like lattice-based cryptography, multivariate cryptography (like the Unbalanced Oil and Vinegar scheme), and even supersingular elliptic curve isogeny cryptography.

These, and other post-quantum cryptography schemes, will have to involve algorithms that are resistant to cryptographic attacks from both (HYBRID) classical and quantum computers, according to the NSA. It’s certain that the threats to privacy and information security will only multiply in the coming decades and that data encryption will proceed with new technological advances. (Dolev, 2018)

Artificial Intelligence as key to future geopolitical power

Russian president Vladimir Putin had in September 2017 addressed 16,000 Russian schools with following statement: „Artificial Intelligence is the future, not only for Russia but for all humankind“, he said via live video beamed to 16,000 selected schools. Then he continued: „Whoever becomes the Leader in this sphere - will become the Ruler of the World“.
There is an intensifying race among USA, Russia and China to accumulate military power based on Artificial Intelligence. All 3 countries have proclaimed intelligent machines a vital to the future of their national security. Technologies such as software that can sift intelligence material or autonomous drones and ground vehicles are seen as ways to magnify the power of human soldiers.

It was published a 132 page report from the Harvard University Belfer Center titled Artificial Intelligence and National Security by Greg Allen and Taniel Chan. A study on behalf of Dr. Jason Matheny, Director of the U.S. Intelligence Advanced Research Projects Activity (IARPA).

Researchers in the field of Artificial Intelligence (AI) have demonstrated significant technical progress over the past 5 years, much faster than was previously anticipated.

- Most of this progress is due to advances in the AI sub-filed of Machine learning.
- Most experts believe this rapid progress will continue and even accelerate.

Existing capabilities in AI have significant potential for national security.

- For example, existing machine learning technology could enable high degrees of automation in labor-intensive activities such as satellite imagery analysis and cyber defense.

Future progress in AI has the potential to be a transformative national security technology, on a par with nuclear weapons, aircrafts, computers, and biotech.

Each of these technologies led to significant changes in the strategy, organization, priorities, and allocated resources of the U.S. national security community. We argue future progress in AI will be at least equally impactful.

Advances in AI will affect national security by driving change in 3 areas: military superiority, information superiority, and economic superiority.

- For military superiority, progress in AI will both enable new capabilities and make existing capabilities affordable to a broader range of actors.

For example, commercially available AI-enabled technology (such as long-range drone package delivery) may give weak states and non-state actors access to a type of long-range precision strike capability.

In the cyber domain, activities that currently require lots of high-skill labor, such as Advanced Persistent Threat operations, may in the future be largely automated and easily available on the black market.

For information superiority, AI will dramatically enhance capabilities for the collection and analysis of data, and also the creation of data.

In intelligence operations, this will mean that there are more sources than ever from which to discern the truth.

AI-enhanced forgery of audio and video media is rapidly improving in quality and decreasing in cost. In the future AI-generated forgeries will challenge the basis of trust across many institutions.

For economic superiority, we find that advances in AI result in a New Industrial Revolution. Former U.S. Treasury Secretary Larry Summers has predicted that advances in AI and related technologies will lead to a dramatic decline in demand for labor such that the USA may have a third of men between the ages of 25 and 54 not working by the end of this half century.

Concerning this topic, in 2017 China State Council released a detailed strategy designed to make the country „the front-runner and global innovation center in AI“ by 2030. It includes pledges to invest in R&D that will „through AI elevate national defense strength and assure protect and national security.


Conclusions
From Frankenstein to, I Robot, we have for centuries been intrigued with and terrified of creating beings that might develop autonomy and free will. And now that we stand on the cusp of the age of ever-more-powerful Artificial Intelligence (AI), the urgency of developing ways to ensure our creations always do what we want them to do is growing. (Seitz, 2018, Siegel, 2018)

In AI, I agree with people like Mark Zuckerberg, with belief that AI will be better in the future. We can solve the problems with AI technology if we will figuring out how to regulate powerful machine-learning-based systems.

The priority of people positively connected with AI become the need to learn more not about just about how Artificial Intelligence work, but how Humans work. Humans are the most elaborately cooperative species on the planet. We outflank every other animal in cognition and communication – tools that have enabled a division of labor and shared living in which we have to depend on others to do their part. That’s what our market economies and systems of government are all about. (Skopec III., 2015, Skopec IV., 2016)

Sophisticated cognition and language – which AIs are already starting to use are the features that make Humans so wildly successful at cooperation. There are also many conservative people which are overvaluing the risks of AIs exercising free will. I am afraid that it is an error turning only to ethicists and philosophers to help think through the challenge of building AI that play nice. (Prigogine, 1997)

Thinkers like Adrienne Mayor, Joann Bryson, Patrick Lin, etc., are wrong with their’s prophecies based on literature from thousands years ago ! Similarly, also Bill Gates and other 115 technological leaders with their threats and menaces from 2017 against development of AIs in military are wrong. The Slovak daily newspapers DennikN, Pravda and Aktuality.sk in Bratislava, Slovakia are propagating old-fashioned, out-dated panic sclerosis from AI for the public too. If your enemies will use the power of the AI and you have not a pre-emptive strategy, then you and your country can be sure that you will be defeated. (Bartels, 2018, Skopec V., 2018)

Social psychologists and roboticists are tinkering about these questions, but we need more research of this type, and more that focuses on a features of the system, not just the design of an individual machine or process. (Skopec V., 2018)

To build smart machines that follow the rules that multiple, conflicting, and sometimes inchoate human groups help to shape, we will need to understand a lot more about the correlations between the Quantum Biology and Artificial Intelligence.

ACKNOWLEDGMENTS

The author gratefully acknowledge the assistance of Dr. Marta Ballova, Ing. Konrad Balla, Livuska Ballova and Ing. Jozef Balla.

References

1. Bartels M: Newsweek, Jan. 5, 2018


30. Zachary Fryer-Biggs Sep 8, 2018, Center for Public Integrity