# Why Banks Should Care More About A.I. Attacks

**Martin Rupp**
SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

Welcome to the 21st century, where science-fiction looks increasingly less like fiction!
A new crypto-threat has emerged from the depths of science and technology, named “neural cryptography."

As with everything disrupting, neural cryptography isn't so new. In 1995, Sebastien Dourlens, a French researcher in cryptography, pioneered it in some ways, including in his master Ph.D. thesis, by using a neural network (quite simple at the time) to perform cryptanalysis of the DES cipher.

Neural cryptography isn't a well-established discipline. It relates to the use of AI and mainly neural networks in cryptanalysis techniques.

The “quantum threat" - e.g., the arrival of mature quantum computers able to crack asymmetric ciphers (among others) could be doubled by the neural threat. For instance, the development of neural network machines could crack even the most sophisticated ciphering algorithms.

## 1 Is There Really a “Neural Threat” in Cryptography?

In his 1995 experiment, Sebastien Dourlens managed to find around 50% of a DES key's bits, therefore considerably reducing the time needed for a brute-force attack. The neural network used a known bias of DES.

However, this doesn't mean that neural networks are specially efficient in cryptanalysis. *It just means that they could be used for the job.*

For instance,successful cryptanalysis of Enigma [1] has been performed using only neural networks. But when compared to traditional cryptanalysis, much more data and power are required. So, is there a neural threat that could break some widely used cryptographic schemes such as AES-256, for instance? The answer has to be mitigated.

Neural networks, especially deep learning, can be very good at identifying the nature of a cipher (AES,3DES, etc.), which should look at “white noise." They could also potentially detect correlations that only these deep learning algorithms are able to “see." Machine learning could crack ciphers when used *combined* with other techniques such as side-channel attacks (see [5]).

AI isn't also limited to deep learning. For example, the technique of generative adversarial networks (GAN) and generally (automatic) game competition between deep neural networks have shown some significant results in neural cryptanalysis.

As with everything with AI, one should be extra careful. Deep learning has dramatically increased its strength with each year since dedicated AI hardware and methods become more and more powerful. Deep learning has its own way, which is extremely different from other "standard" algorithms. The way that neural networks operate is partly a mystery and the research in this area is often more a question of intuition, experience, and trial and error than the result of a synthetic scientific theory!

In the paper "Neuro-Cryptanalysis of DES and Triple-DES" [2], the author claims to have successfully achieved some significant results on the cryptanalysis of 3DES using neural networks. This is also linked with results published in [3].

Given a ciphertext, a neural network could potentially predict which one, among several candidates, has the most chance of being the corresponding plaintext. In general, this is more coherent with the logic of AI.

For instance, [3] uses image classification on encrypted data and reaches a score of 42%. This is significant compared to the 10% obtained by a random classification.

This may indicate that while neural networks are still not able to break modern ciphers such as 3DES or AES, they seem to extract significant information from them, even if there is very little research (at least publicly available) over this. This should be perceived as a real threat by actors such as banks. A neural network may be able to break the 3DES cipher in the relatively near future.

## 2 Overview of Some Neural Cryptographic Algorithms

Historically, Lauria [4] is one of the first researchers to have introduced the concept of neural-network powered cryptography as soon as 1990. Using neural network algorithms for cryptography may prevent neural cryptanalysis from being used successfully against ciphers. Currently, there are AES implementations using deep learning networks.

The neural key exchange protocol, using chaos theory, is a first try to propose neural network-based key exchange protocols. While imperfect, it could lead to a version of cryptography using continuous variables (instead of the current one which is discrete).

Generally speaking, neural crypto algorithms should be resistant to linear cryptanalysis, one of the most common forms of cryptanalysis. They should also be resistant to neural cryptanalysis, of course.

### 2.1 Towards Neural Crypto Proof Algorithms

If there is a neural threat, then are there some "neural crypto proof" algorithms?
It is hard to say for the moment. The situation is different from the quantum crypto threat.
AI-resistant cryptographic algorithms may be much harder to create than the quantum proof ones.

This is a new domain where banks should stay focused on since their cryptographic systems rely heavily on RSA, AES, and 3DES, which are currently actively targeted by neural cryptography.

### 2.2 The need for crypto-agile security infrastructures

For sure, the coming years will require regular revisiting of the crypto-algorithms in use. We will need to proceed in a crypto-agile way. Acting proactively and at the same time driven by new research results, adapting policies, experiences made and evolving regulations, security-sensitive organizations need to be able to respond rapidly.

The prerequisite for this is a crypto-agile infrastructure, allowing for changes conducted from a central control center in a minimum period of time and with limited financial and HR resources involved.

[1] Learning the Enigma With Recurrent Neural Networks, S Greydanus. 2017
[2] Neuro-Cryptanalysis of DES and Triple-DES , Mohammed M. Alani. 2012
[3] Extracting Information from Encrypted Data using Deep Neural Networks. Lagerhjelm . 2019
[4] On neurocryptology. Lauria, F. E. 1990.
[5] Side-Channel Analysis of AES Based on Deep Learning, Huanyu Wang. 2019