Counterterrorism for Cyber-Physical Spaces: A Computer Vision Approach

Giuseppe Cascavilla
Eindhoven University of Technology
Den Bosch, Netherlands
g.cascavilla@tue.nl

Johann Slabber
Tilburg University
Den Bosch, Netherlands
j.slabber@tilburguniversity.edu

Fabio Palomba
SeSa Lab - University of Salerno
Salerno, Italy
fpalomba@unisa.it

Dario Di Nucci
Tilburg University
Den Bosch, Netherlands
d.dinucci@uvt.nl

Damian A. Tamburri
Eindhoven University of Technology
Den Bosch, Netherlands
d.a.tamburri@tue.nl

Willem-Jan van den Heuvel
Tilburg University
Den Bosch, Netherlands
W.J.A.M.v.d.Heuvel@jads.nl

ABSTRACT

Simulating terrorist scenarios in cyber-physical spaces—that is, urban open or (semi-) closed spaces combined with cyber-physical systems counterparts—is challenging given the context and variables therein. This paper addresses the aforementioned issue with AL$_{Ter}$ a framework featuring computer vision and Generative Adversarial Neural Networks (GANs) over terrorist scenarios. We obtained the data for the terrorist scenarios by creating a synthetic dataset, exploiting the Grand Theft Auto V (GTAV) videogame, and the Unreal Game Engine behind it, in combination with OpenStreetMap data. The results of the proposed approach show its feasibility to predict criminal activities in cyber-physical spaces. Moreover, the usage of our synthetic scenarios elicited from GTAV is promising in building datasets for cybersecurity and Cyber-Threat Intelligence (CTI) featuring simulated video gaming platforms. We learned that local authorities can simulate terrorist scenarios for their cities based on previous or related reference and this helps them in 3 ways: (1) better determine the necessary security measures; (2) better use the expertise of the authorities; (3) refine preparedness scenarios and drills for sensitive areas.

CCS CONCEPTS

• **Human-centered computing → Visualization systems and tools**.

KEYWORDS

Cyber-Physical Spaces, Counterterrorism, Computer Vision, Generative Adversarial Neural Networks

ACM Reference Format:
Giuseppe Cascavilla, Johann Slabber, Fabio Palomba, Dario Di Nucci, Damian A. Tamburri, and Willem-Jan van den Heuvel. 2020. Counterterrorism for Cyber-Physical Spaces: A Computer Vision Approach. In *International Conference on Advanced Visual Interfaces (AVI '20), September 28-October 2, 2020, Salerno, Italy.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3399715.3399826

1 INTRODUCTION

While the world has never been safer from criminal phenomena such as terrorism than today, the news seems to be dominated by headlines of violent assaults [30]. Urban spaces are vulnerable places as they can be attacked with simple methods and at low costs and preparation. Consequently, authorities trying to protect such open urban (soft) targets are faced with innumerable, and rather unpredictable, attacks. This poses enormous challenges for cities, security authorities and enforcement units. At the same time, these actors are typically constrained in their resources including their expertise and experience. This is especially true in smaller cities, where law enforcement agencies typically lack proper knowledge, infrastructure, and supporting (costly) technology to be fully prepared for these events in terms of vulnerability assessments and contingency plans [20].

To address the above considerations, this paper reports on the investigation on how -and to which extend- computer vision approaches can help law-enforcement agencies and municipalities in the protection of urban spaces against terrorism [26]. On the one hand, our goal is to inform law-enforcement agents (LEAs) about the potential impact of these attacks on the locations they protect. On the other hand, we aim at simulating the behaviour that the agents should have to most effectively fight them, reducing the impact of incidents.

To this end, we have designed, explored and prototyped AL$_{Ter}$—**A**dversarial **L**earning for counter**Ter**rorism—a novel framework to simulate complex terrorism scenarios based on the synthesis of computer vision and deep learning. The purpose of AL$_{Ter}$ is three-fold. Firstly, the AL$_{Ter}$ solution helps LEAs to identify vulnerable locations in urban areas (such as entrances) and prepare appropriate responses and contingency plans [12]. Secondly, AL$_{Ter}$ provides city policy-makers a simulation of the consequences that attacks could have in specific areas of public spaces, hence giving the LEAs and municipalities the possibility to predict, manage, and avoid terrorist attacks with a surgically-precise lens of analysis. Thirdly, and finally, AL$_{Ter}$ would allow local law-enforcement

AVI '20, September 28-October 2, 2020, Salerno, Italy
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-7535-1/20/09…$15.00
https://doi.org/10.1145/3399715.3399826

agencies to provide landmark images from their location and simulate different scenarios that occurred in other locations, thus enabling the actionable use of counter-terrorism information sharing for preparedness and urban contingency-planning beyond terror-understanding. Our computer vision approach trains Generative Adversarial Networks [17] using images of terrorist attacks extracted from video-gaming scenarios. In the scope of AL_{Ter}, GANs are used as a key design artefact since they were previously used to reproduce fake images which are almost indistinguishable to real ones (e.g., deep fakes) [16] and therefore we assumed they may be equally suitable to be applied to terrorist attack simulation as well.

To the best of our knowledge, AL_{Ter} is the first attempt in this direction. To demonstrate its feasibility, we implemented a proof-of-concept and simulated terrorist attacks via gamification [18]. In particular:

- we mined criminal action videos from Grand Theft Auto V[1];
- we elicited information from OpenStreetMap[2] (OSM) to simulate an event in a real location;
- we use StyleGAN [22] to map the features of the extracted terrorist attack scenes to the latent space.
- we changed such latent space to extract terrorist attacks (e.g., a vehicle ramming humans in an image) and transfer them to other locations.

We evaluate our proof-of-concept in the real-world scenario of the city of Malaga (ES) in which we simulated a small scale terrorist attack (i.e., a terrorist starting a fire in the main square of the city). The primary goal of our evaluation was to assess the extent to which we could transfer the scenarios from a simulated environment to the real-world cyber-physical spaces counterparts existing in the same city. The contributions of this paper are:

1. a computer vision framework to simulate terrorist attacks in other locations;
2. a proof-of-concept featuring StyleGAN to implement such framework;
3. an initial evaluation of the StyleGAN architecture [23] in the context of terrorist attack simulations.

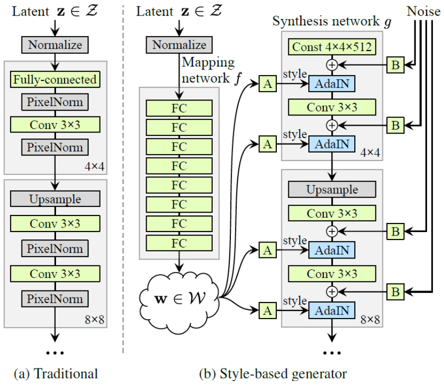
The remaining of the paper is organized as follows. Section 2 presents the technologies used in this paper. Section 3 outlines the problem definition, the framework, and the data required by the approach. Section 4 reports on the proof-of-concept, while Section Section 5 concludes the paper.

2 BACKGROUND

Computer vision is a branch of Artificial Intelligence (AI), which focuses on partially replicating the complexity of human vision systems to enable computers to identify and process objects in images and videos in the same way that humans do. In this research paper, we present a computer vision approach to give to municipalities and local law enforcement agencies a new tool to prevent and minimize the effects of terrorist attacks. In this section, we describe (i) how artificial intelligence can be used to model criminal scenarios and (ii) generative adversarial networks for computer vision.

2.1 AI to Model Criminal Scenarios

Conte et al. [7] use Artificial Intelligence (AI) to model complex scenarios. To generate data regarding criminal activities, usually, multi-agent-based simulations are used [4, 8, 19]. Bosse et al. [4] and Hao et al. [19] identify targets for burglary and other criminal activity. Devia and Weber [8] evaluated the performance of current practices to reduce the resources required by a city. More recently, Birks et al. [3] criticized the top-down approach for analyzing crime. They argued that researchers should exploit computational models and the interactions between the different components of dynamic social systems to investigate the effect of manipulating such components. The current state-of-the-art for analyzing terrorism scenarios focuses on risk assessment, which is based on regression models and probability theory [11, 24]. However, these approaches can lead to misleading results as terrorist activities are surrounded by high uncertainty [6]. Currently, there is no successful approach to simulate terrorist scenarios by considering all the different parameters that entail a terrorist attack.



(a) Traditional

(b) Style-based generator

Figure 1: Difference a traditional and a style-based generator architecture from Karras et al. [22].

2.2 GAN and Computer Vision

To simulate terrorist scenarios, we rely on Generative Adversarial Networks [17] (GANs). The ability of GANs in generating realistic images has rapidly increased in recent years. The concept of transferring the content of an image to another one has been initially introduced by Gatys et al. [15].

BigGANs have been introduced by Brock et al. [5] and improve GANs in terms of scalability, robustness, and stability. BigGANs are suitable to encode diverse pictures by isolating the different aspects of the images. This approach is suitable for modelling complex scenarios such as terrorist attacks. However, the network size prevented us to apply this network due to the huge computing power needed to train the model. Therefore, we relied on StyleGANs, a new architecture proposed by Karras et al. [22] that combines GANs and AdaIN and was successfully applied to other domains than paintings [14].

Figure 1 depicts the differences between the style-based generator architecture and the traditional GANs. StyleGAN extends the progressive training with a mapping network with to goal of

[1] https://www.rockstargames.com/V/
[2] https://www.openstreetmap.org/

encoding the input into a feature vector whose elements control different visual features and styles that translate the previous vector into its visual representation. By using separate feature vectors for each level, the model can combine multiple features. With respect to other equally effective GANs (e.g., BigGANs [5]), this model requires less training time to produce high-quality realistic-looking images [31].

3 TOWARDS ALTER: COMPUTER VISION FOR COUNTERTERRORISM SIMULATION

As previously mentioned, this paper elaborates ALTer, a framework to describe the elements needed to simulate the protection of public cyber-physical space against terrorism. Previous work already established that due to the high dimensionality of the involved variables this problem is complex [27]. In particular, we describe the *data* that should feed the *simulation* implemented by GANs.

3.1 Framework Parameters

Based on previous work [4], we analyzed the factors that should be considered in the simulation of counterterrorism on public spaces. Table 1 lists the parameters we elicited from the state of the art grouped in categories namely: (i) the *Environment* where the terrorist attack happen, (ii) the *Event* happening in the environment, and (iii) the *Agents* that move in the environment.

Environment	
Location	3D composition of the location of the main site, including all the buildings and access areas
# of Entries	number of places that people are able to enter the main site
# of Exits	number of places that people are able to exit the main site
# Access Control	number of secured entry points
# of Barriers	number of access points with barricades (including natural ones) to protect against the attack
Surveillance	if there are surveillance systems in place for early alerting against an attack
Event	
Activity	the type of event that is taking place
Attack	the type of attack
Crowd Density	how many people per square meter will be at the event
Agents	
Type	citizens = people attending the event or which are in close proximity, these are the targets of terrorists terrorist = a criminal attack on citizens, with the intent of inflicting death or serious bodily injury police = police officers (either on foot or in a vehicle) which are responsible for protecting citizens fire and rescue = firefighters/rescue personal which are part of emergency response health = ambulances and hospitals which are responsible for emergency response in case when people are injured
Groups	groups of agents (e.g., police agents or families) should be together
Speed	the speed of the agent
Vision Radius	the distance in which an agent is able to detect another agent
Route	route that the agent follows
Response Time	the response time of agent

Table 1: Parameters needed for counterterrorism simulation.

Environment. The environment reflects the place where the event takes place. It entails the entire cyber-physical terrain, the security measures, and the cyber-tech which are in place and interacting with the terrain itself (e.g., fixed-cams, drones, aerial recognition intelligence, etc.).

Event. The event describes the type of terrorist scenario, the activity that was taking place during the attack, and the crowd density.

Agents. Agents are all the different individuals that we consider in the simulation. As described in Table 1, there are five types of agents. A single scenario should be composed at least of (i) the citizens who are in the environment, (ii) the terrorist who is are attacking the main site, and (iii) the emergency services (i.e., police, fire and rescue, and health). Each agent has a certain speed that for example could be determined by the means of transportation.

3.2 Using Generative Adversarial Networks to Protect Cyber-Physical Spaces

After defining the framework parameter, we need to successfully train the Generative Adversarial Network to encode the world inside the network. With this respect Bau et al. [2] showed that it is possible to map specific components of images back to causal units inside the layers of a GAN. Specifically, they used segmentation masks to effectively distinguish between trees or humans and map them back to the layers of the network. They also showed that by adjusting the network they could force it to generate a door an place it on a building. Once the GAN has been successfully trained, the next step is to reverse the GAN to map the image features back to their variables in their latent representation. Donahue et al. [9] and Dumoulin et al. [10] proposed an encoder to map the created images back to their representation in the latent space. Alternatively, Luo et al. [25] introduced inverse mapping and reformulated the problem as a minimization problem. For sake of simplicity, please consider that neural networks have three basic components: (i) input, (ii) parameters, and (iii) output of the network. In our framework, we keep the input and output fixed, and we map the parameters through backpropagation from the input to output differently from Luo et al. [25] who keep the output and parameters fixed and map the output images back to the latent input vector. To implement scalable GAN, we could rely on BigGANs [5] and StyleGANs [22]. However previous research [1, 13, 29] showed that StyleGANs are more suitable for large datasets, hence motivating our choice towards such networks.

4 PROOF OF CONCEPT

An initial part of the defined above framework has been implemented in a proof of concept, which we describe and preliminarily evaluated in the following sections. The goal of this proof of concept is to demonstrate that it is possible to use Generative Adversarial Networks to transpose an *event* in a different *environment.*

4.1 Prototype Implementation

Figure 2 shows the AL$_{Ter}$ pipeline to extract the data needed to feed and train the Generative Adversarial Network: the environment and the event.

Retrieving the Environment. To retrieve the data concerning the environment, we collect and assemble multiple images that represent real-world sites, i.e., the environment on which our approach should be applied to predict criminal activities. To this aim, several steps are required:

(1) Create a low-quality representation of the environment using the Unreal engine[3]

[3] https://www.unrealengine.com/

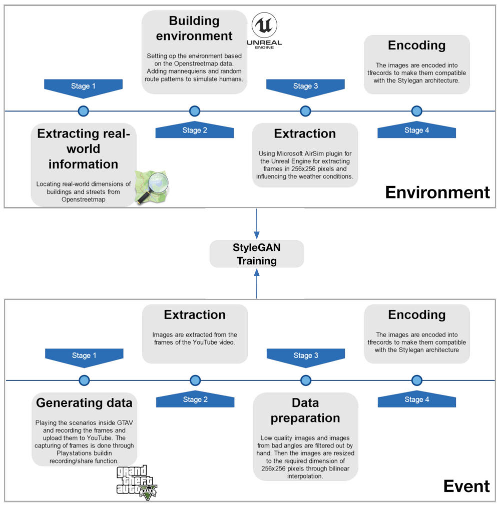

Building environment
Setting op the environment based on the Openstreetmap data. Adding mannequiens and random route patterns to simulate humans.
UNREAL ENGINE
Encoding
The images are encoded into tfrecords to make them compatible with the Stylegan architecture.
Stage 1
Stage 2
Stage 3
Stage 4
Extracting real-world information
Locating real-world dimensions of buildings and streets from Openstreetmap
Extraction
Using Microsoft AirSim plugin for the Unreal Engine for extracting frames in 256x256 pixels and influencing the weather conditions.
Environment
StyleGAN Training
Extraction
Images are extracted from the frames of the YouTube video.
Encoding
The images are encoded into tfrecords to make them compatible with the Stylegan architecture
Stage 1
Stage 2
Stage 3
Stage 4
Generating data
Playing the scenarios inside GTAV and recording the frames and upload them to YouTube. The capturing of frames is done through Playstations buildin recording/share function.
grand theft auto FIVE
Data preparation
Low quality images and images from bad angles are filtered out by hand. Then the images are resized to the required dimension of 256x256 pixels through bilinear interpolation.
Event

Figure 2: AL_{Ter} Pipeline: environment (top) and events (bottom) extraction, and training of GAN.

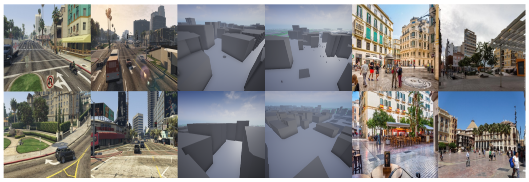


Figure 3: GTAV urban spaces (left), skeleton representations of Malaga (centre), four real locations in Malaga (right).

(2) Acquire the information concerning the building size and dimensions from Openstreetmap[4] and add some basic mannequins;
(3) Extract frames of 256x256 pixels using the Microsoft AirSim plugin [28];
(4) Encode the frames within the StyleGan architecture.

Examples of these simulations can be found in Figure 3 which represent several squares in Malaga (Spain)

Generating and Collecting Events. The second step toward this proof of concept concerns the events. We exploit GTAV and collect data coming from several gameplay sessions recorded from different perspectives. Overall, we collect around 10, 000 images which have elements involving terrorist attacks from multiple views which even includes a helicopter filming a truck ramming into people/buildings. For testing whether the network can distinguish the features of terrorist attacks, we use another dataset which contains sequences of urban spaces of GTAV and was previously employed by Huang et al. [21]. This dataset provides to us unseen images that we could use in the interpolation operations to test the disentanglement. Figure 2 shows the steps required to extract the data. To simulate counterterrorism events, the following main steps are required:

(1) Play and record gaming scenarios;
(2) Extract the frames for such videos;
(3) Post-process the frames to remove clutter and reduce their resolution to 256x256 pixels;
(4) Encode the frames within the StyleGan architecture.

Training the Generative Adversarial Network. To model the *simulation*, we rely on StyleGAN architecture. We consider this model as a black box as we do not have control over how it learns the elements of the scenario. As for the loss function, apriori we do not know which one works best for a two-fold reason: there is no previous research which encoded real-world images to synthetic datasets and previous experiments were not in the context of terrorist scenarios. Therefore, we considered a combination of several loss functions considered in the state-of-the-art: (i) Pixel-wise loss, (ii) MS-SSIM loss, (iii) LPSIS loss, and (iv) VGG loss.

To converge, a GAN requires that the output of the loss function for both the generator and the discriminator are around -0.5 and 0.5 in terms of Mean Squared Error (MSE). During the training phase, we observed that training low-resolution layers is easier than training higher quality layers. An example is provided in Figure 4, where the Y-axis is the loss and the X-axis is the number of steps the network trained. Here the loss gradually moves towards the targeted loss until the network switches to a higher resolution: from that point the loss moves in the opposite direction.

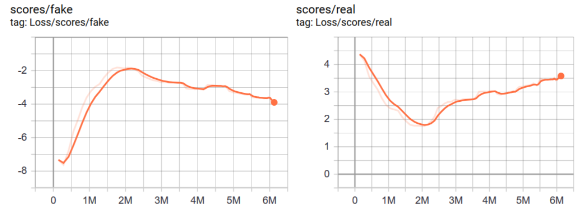


Figure 4: Loss progress while training on the events generated with GTA V with a resolution of 256px.

We analyzed the reasons behind the issue and we discovered that the network is not able to converge due to the diversity of the images in the event dataset. Hence we decided to train the network using only the images from the dataset by Huang et al. [21]. We observed that when increasing the quality of the images, the training session tends to break down as well. Finally, we retrained the network on a dataset created from the Unreal engine in which some mannequins representing people were running around the environment. To simulate an attack, we included a fire in a random location of the square. The images of this dataset were less diverse and generally of the same shape. Furthermore, the initial location was encoded as a set of blocks. To diversify the dataset, we included several images of squares in the city of New York as well. The network did converge smoothly to the target loss of -0.5/0.5 as is shown by the loss graphs in Figure 5.

4.2 Limitations and Lessons Learned

Feature Spatial Location. The network not always can effectively disentangle all features within the latent code. This constitutes an additional challenge for Generative Adversarial Networks.

Loss Functions. None of the loss function is suitable to model complex simulations such as terrorist attacks.

[4] https://www.openstreetmap.org/

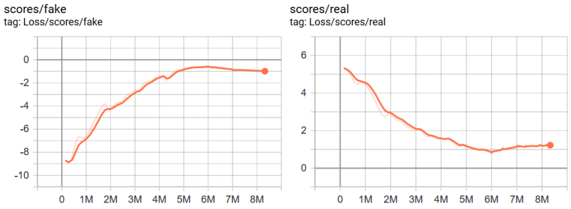


Figure 5: Loss progress while training on the events generated with the Unreal Engine.

Alternatives to StyleGANs. The network cannot cope with high diversity. In other words, StyleGANs seem not being able to isolate the different aspects of the images. However, BigGANs could be a suitable alternative that we will analyse as part of our future agenda.

5 CONCLUSIONS

In this paper, we introduced AL$_{Ter}$, a framework for Law Enforcement Agencies to simulate real-life terrorist attack scenarios in their cities to support several counter-terrorism and crime-fighting activities, e.g., a better-instrumented preparedness plan to counter terrorist attacks. Our approach and tool feature a novel way for simulating terrorism scenarios by using computer vision and GANs, that is, generative adversarial neural networks that learn automatically the features of terrorist scenarios and can simulate such features in the scope of real-life cyber-physical systems and spaces.

Our proof-of-concept shows we could simulate real-life cyber-physical spaces as subject to terrorist threats, but we were not able to do so effectively and with a low margin of error. However, our proof-of-concept shows that the future of this approach is promising and further experimentation is needed, possibly with different architectures, more data and better quality data as well as data-fusion approaches between real and simulated data. Furthermore, as part of this study, we show a new way of generating data for terrorism scenarios based on video-gaming, thus addressing the lack of data and the sensitivity criticalities around terrorism data.

ACKNOWLEDGMENTS

This paper was funded by the European Union's Internal Security Fund — Police under grant agreement n° 815356. Palomba acknowledges the support of the Swiss National Science Foundation through the SNF Project No. PZ00P2_186090 (TED).

REFERENCES

[1] Rameen Abdal, Yipeng Qin, and Peter Wonka. 2019. Image2StyleGAN: How to Embed Images Into the StyleGAN Latent Space? arXiv:cs.CV/1904.03189

[2] David Bau, Jun-Yan Zhu, Hendrik Strobelt, Bolei Zhou, Joshua B. Tenenbaum, William T. Freeman, and Antonio Torralba. 2018. GAN Dissection: Visualizing and Understanding Generative Adversarial Networks. arXiv:cs.CV/1811.10597

[3] Daniel Birks, Michael Townsley, and Anna Stewart. 2012. Generative explanations of crime: Using simulation to test criminological theory. *Criminology* 50, 1 (2012), 221–254.

[4] Tibor Bosse and Charlotte Gerritsen. 2009. Comparing crime prevention strategies by agent-based simulation. In *2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology*, Vol. 2. IEEE, 491–496.

[5] Andrew Brock, Jeff Donahue, and Karen Simonyan. 2018. Large Scale GAN Training for High Fidelity Natural Image Synthesis. arXiv:cs.LG/1809.11096

[6] Gerald G Brown and Louis Anthony Cox, Jr. 2011. How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Analysis: An International Journal* 31, 2 (2011), 196–204.

[7] Rosaria Conte, Rainer Hegselmann, and Pietro Terna. 2013. *Simulating social phenomena*. Vol. 456. Springer Science & Business Media.

[8] Nelson Devia and Richard Weber. 2013. Generating crime data using agent-based simulation. *Computers, Environment and Urban Systems* 42 (2013), 26 – 41. https://doi.org/10.1016/j.compenvurbsys.2013.09.001

[9] Jeff Donahue, Philipp Krähenbühl, and Trevor Darrell. 2016. Adversarial feature learning. *arXiv preprint arXiv:1605.09782* (2016).

[10] Vincent Dumoulin, Ishmael Belghazi, Ben Poole, Olivier Mastropietro, Alex Lamb, Martin Arjovsky, and Andrew Courville. 2016. Adversarially learned inference. *arXiv preprint arXiv:1606.00704* (2016).

[11] Barry Charles Ezell, Steven P Bennett, Detlof Von Winterfeldt, John Sokolowski, and Andrew J Collins. 2010. Probabilistic risk analysis and terrorism risk. *Risk Analysis: An International Journal* 30, 4 (2010), 575–589.

[12] Stanley Friedman. 1982. Contingency and disaster planning. *Computers & Security* 1, 1 (1982), 34–40.

[13] Aviv Gabbay and Yedid Hoshen. 2019. Style Generator Inversion for Image Enhancement and Animation. *arXiv preprint arXiv:1906.11880* (2019).

[14] Leon A. Gatys, Alexander S. Ecker, and Matthias Bethge. 2015. A Neural Algorithm of Artistic Style. *CoRR* abs/1508.06576 (2015). http://arxiv.org/abs/1508.06576

[15] Leon A Gatys, Alexander S Ecker, and Matthias Bethge. 2016. Image style transfer using convolutional neural networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition.* 2414–2423.

[16] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2014. Generative Adversarial Nets. In *Advances in Neural Information Processing Systems 27*, Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger (Eds.). Curran Associates, Inc., 2672–2680. http://papers.nips.cc/paper/5423-generative-adversarial-nets.pdf

[17] Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2014. Generative Adversarial Networks. http://arxiv.org/abs/1406.2661 cite arxiv:1406.2661.

[18] J. Hamari, J. Koivisto, and H. Sarsa. 2014. Does Gamification Work? – A Literature Review of Empirical Studies on Gamification. In *2014 47th Hawaii International Conference on System Sciences*. 3025–3034. https://doi.org/10.1109/HICSS.2014.377

[19] Mengmeng Hao, Dong Jiang, Fangyu Ding, Jingying Fu, and Shuai Chen. 2019. Simulating Spatio-Temporal Patterns of Terrorism Incidents on the Indochina Peninsula with GIS and the Random Forest Method. *ISPRS International Journal of Geo-Information* 8, 3 (2019), 133.

[20] Isaias Hoyos, Bruno Esposito, and Miguel Núñez del Prado. 2018. DETECTOR: Automatic Detection System for Terrorist Attack Trajectories.. In *SIMBig (Communications in Computer and Information Science)*, Juan Antonio Lossio-Ventura, Denisse Muñante, and Hugo Alatrista-Salas (Eds.), Vol. 898. Springer, 160–173.

[21] Po-Han Huang, Kevin Matzen, Johannes Kopf, Narendra Ahuja, and Jia-Bin Huang. 2018. DeepMVS: Learning Multi-View Stereopsis. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR).*

[22] Tero Karras, Samuli Laine, and Timo Aila. 2019. A Style-Based Generator Architecture for Generative Adversarial Networks. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR).* https://github.com/NVlabs/stylegan

[23] Tero Karras, Samuli Laine, Miika Aittala, Janne Hellsten, Jaakko Lehtinen, and Timo Aila. 2019. Analyzing and Improving the Image Quality of StyleGAN. *CoRR* abs/1912.04958 (2019).

[24] Jingyu Liu, Walter W Piegorsch, A Grant Schissler, and Susan L Cutter. 2018. Autologistic models for benchmark risk or vulnerability assessment of urban terrorism outcomes. *Journal of the Royal Statistical Society: Series A (Statistics in Society)* 181, 3 (2018), 803–823.

[25] Junyu Luo, Yong Xu, Chenwei Tang, and Jiancheng Lv. 2017. Learning inverse mapping by autoencoder based generative adversarial nets. In *International Conference on Neural Information Processing*. Springer, 207–216.

[26] Vivek Menon, Bharat Jayaraman, and Venu Govindaraju. 2011. The Three Rs of Cyberphysical Spaces. *IEEE Computer* 44, 9 (2011), 73–79.

[27] Il-Chul Moon and Kathleen M. Carley. 2007. Modeling and Simulating Terrorist Networks in Social and Geospatial Dimensions. *IEEE Intelligent Systems* 22, 5 (2007), 40–49.

[28] Shital Shah, Debadeepta Dey, Chris Lovett, and Ashish Kapoor. 2017. AirSim: High-Fidelity Visual and Physical Simulation for Autonomous Vehicles. In *Field and Service Robotics*. arXiv:arXiv:1705.05065 https://arxiv.org/abs/1705.05065

[29] Yujun Shen, Jinjin Gu, Xiaoou Tang, and Bolei Zhou. 2019. Interpreting the latent space of gans for semantic face editing. *arXiv preprint arXiv:1907.10786* (2019).

[30] Dimitris Spiliotopoulos, Costas Vassilakis, and Dionisis Margaris. 2019. Data-driven country safety monitoring terrorist attack prediction.. In *ASONAM*, Francesca Spezzano, Wei Chen, and Xiaokui Xiao (Eds.). ACM, 1128–1135.

[31] Kayo Yin. 2019. How to Train StyleGAN to Generate Realistic Faces. https://bit.ly/2FQ0CU7.