Stefan Werning

The Convergent Use of Programmable Media for Terrorism Modeling and Social Simulations in Civilian vs. Military Contexts

2008

https://doi.org/10.25969/mediarep/1562

Veröffentlichungsversion / published version
Sammelbandbeitrag / collection article

Stefan Werning

The Convergent Use of Programmable Media for Terrorism Modeling and Social Simulations in Civilian vs. Military Contexts

Modeling Terrorism as a Household Strategy

The rhetoric of the ›Global War on Terrorism‹ is a recurring theme in interactive, i.e. programmable media like digital games (cf. e.g. commercial games like FUGITIVE HUNTER: WAR ON TERROR (Black Ops Entertainment, 2003) and WAR ON TERROR (Digital Reality, 2006)) and on-line portals establishing the ›War on Terrorism‹ as a quasi-›brand‹ in public discourse. ◂1 Technological developments enabling the algorithmic modeling of terrorism are a central strategic component both of modern military self-description, e.g. following the ›information warfare‹ paradigm, and of civilian applications, leading to a reversal of Friedrich Kittler's famous dictum pointing at the military roots of entertainment and visualization technologies.

The convergence of civilian and military applications of programmable media, including the exchange of technology between commercial computer games like FULL SPECTRUM WARRIOR (Pandemic Studios, 2004) and projects developed by the US Department of Defense's think tanks like the Institute for Creative Technologies (ICT) and the Defense Advanced Research Projects Agency (DARPA), reveals a blurring of binarisms like the civilian/military distinction and an at least latent militarization, e.g. in terms of language use, collective imaginary and (para)social organization. This goes beyond positive representation and use of military iconography and refers to programmable media use creating collective patterns of thinking compatible with military agendas. To approach this complex phenomenon, the military strategy of algorithmic modeling can be regarded as an iconic characteristic of the Global War on Terrorism. As I attempt to demonstrate in this article, it is inherently plausibilized by digital games and technologically similar programmable media genres.

As a first premise, I understand digital games primarily as programmed/programmable media since the structural paradigm of program code, most notably object-oriented programming (OOP), employed in most current programmable media contexts both pre-forms what can be algorithmically represented and produces recurring representational patterns. Shifting the focus from

game-specific aspects like player identification or the tension between narrative and rule system towards instances of technological convergence allows for meaningful synchronous as well as diachronic cross-references. Taking this a step further, programming practices like code reuse and tool design (e.g. in the form of licensable game engines) need to be analyzed semiotically as instances of producing and modifying signification which are gradually naturalized.
Thus, while this article focuses on military-related game examples, the hypotheses explored herein are similarly applicable to any form of digital games or other programmable media. The article therefore is not primarily concerned with a specific strategy but rather with the preconditions for strategic thinking in times of programmable media.
The mathematicization of terrorism has already been explored at earlier times with respectively different premises; while a historically comparative perspective on the modeling of terrorism could certainly be valuable to obtain a broader perspective on its rootedness in both politico-historical and technological developments, a few brief remarks must suffice for now.
A study dating back to 1981 offers a typology of »terrorist event[s]« and a formal game model for appropriate government reactions (cf. Corsi 1981, 47). The most blatant differences to the current situation are the focus on hostage taking as the contemporary paradigm for terrorist activities (likely after the Iran Hostage Crisis from 1979-81) and the proposition to identify optimal bargaining strategies for governments, alluding to a political environment in which negotiation was standard governmental practice and which appears quite › historicized‹ from today's perspective.
The argument type of the typology can be seen in many ways as a conceptual precursor to the current focus on simulations. It is quasi-interactive in that it allows for the theoretical transformation of complex ›input data‹ into ordered ›output‹ similar to the more recent examples discussed briefly in this article.
In this article, I will attempt to tie the rather abstract technological developments back to concrete examples, both of military applications and commercial digital games like e.g. COMBAT MISSION: SHOCK FORCE (Big Time Software, 2007); for this purpose, a critical reading of designer diaries and technical documents can be one important technique to derive practices and verify hypotheses (for one such documentation cf e.g. Grammont 2007).
According to an interview predating the release of the game, a particular approach was used to identify and outline possible conflicts as scenarios for the upcoming game, a technique which could be rephrased as ›mental simulation‹. As I will argue in more detail later, this process can be understood as inherently ludic. The overall goal thereby was to come up with a plausible conventional

weapons conflict set in the Middle East and involving the U.S. as one faction; this scenario was then implemented into the final game. The actual decision was found by ›playing out‹ and mentally extrapolating hypothetical scenarios and comparing the results, i.e. performing an iterated simulation, a practice similar to those naturalized by programmable media (Grammont 2007, 1). The playfulness of this approach stems in part from abandoning military logic in the scenario selection, i.e. going for a conventional warfare scenario in the first place although aerial operations would be much more likely in reality.

The ›mental simulation‹ in this example is much more complex than one would expect of a digital game design process, e.g. delineating the assumed troop sizes and armament quality of the factions involved, and exhibits the type of encyclopaedic thinking which is, at least partially, the result of working with databases and other programmable media tools indebted to what Lev Manovich tentatively termed ›database logic‹.

The semi-fictional U.S. military campaign focusing on conventional warfare in Combat Mission: Shock Force was modelled on the so-called Stryker brigade, (Grammont 2007, 2) a lightly armoured, highly mobile unit that was built around the ›Stryker‹ combat vehicle and assembled only a few years ago for deployment in Iraq and elsewhere. The Stryker vehicle, as elaborated in the designer diary, focuses on a very efficient communication system that ensures a constant flow of information »up and down the chain of command«. (Grammont 2007, 2) Again, as I will elaborate later, this actual military constellation referenced in the game can be theorized as a manifestation of principles inferred by the pervasive use of programmable media in military contexts, most prominently the principles of OOP with every Stryker unit as an ›object‹.

The focus on semi-autonomous, highly flexible and interconnected (but lightly armoured) ›agents‹ represents a clear departure from earlier paradigms of military strategy and perfectly maps onto the structure of enabling technologies; therefore, it is immediately plausible that a digital game aiming for perceived authenticity would take up this element which is easily representable with the given technologies.

It should be noted that the game engine used for Combat Mission: Shock Force was originally designed for strategy games set in World War II and reprogramming the engine necessarily involved a rethinking of the continuities and ruptures between the conflicts it was and is designed to depict, both on behalf of the developers and, as a proxy, the players who are usually equipped with that background knowledge and implicitly uncover (or, more precisely, ›reverse-engineer‹) the technological setup through the designer diaries and other forms of documentation as part of their media usage. (This element of ›demystification‹ was e.g. described in Friedman, 1999) One particularly characteristic modification is the fact that one »human figure in the game« (Grammont 2007, 3) now only represents a single soldier rather than a small troop; this iconic relationship is but one fairly commonsensical shift in the units of measurement used in actual military strategy that can be mapped to its underlying technological framework and is taken up in quasi-fictional representations.

Before taking a closer look at the manifold relations between terrorism modeling, programmable media technologies like digital games and the logic behind some current political directions, two brief clarifying comments are in order. First, both contextualist and deterministic histories of technology need to be taken into account to obtain an accurate picture; however, due to the scope of this article, I will focus on the recently less covered deterministic perspective and occasionally hint at the mutual shaping of technologies and their social usage. Second, the article offers numerous bibliographical references rather than focusing on few formative texts which is intentional since the overall objective was to give an overview of this generalizable phenomenon, sketch some dominant traits, and provide conceptual entry points for further inquiry.

Programmable Media Strategies for the War on Terror

My main working hypothesis thus holds that the politico-military reliance on agent-based modeling readily translates into actual policies and military decision-making which are gradually plausibilized by programmable media like digital games. One way to approach and verify this claim could be to consider the increasing visibility of MOUT-type (military operations in urban terrain) situations both in military training and commercial games. (for a brief overview of MOUT relevance after 9/11, cf. e.g. McDonald 2003) Certainly, this overlap is partially due to the topicality of urban combat theaters which usually ensures enough familiarity for a digital game to achieve notable commercial success. On the other hand, however, concurrent technological developments like research into team AI in close quarters is another reason for the common theme.

Through the repeated and automatable use of training tools, issues like cultural differences need to be algorithmically expressible and, thus, are discretely defined as »a set of cultural challenges« that needs to be mastered using »cultural awareness training«. (McDonald 2003, 24) Naturally, using distributed AI agents in a simulation to metonymically stage ›cultural specificities‹ must result at least in a partial respective understanding of culture as emergent behavior, i.e. the aggregate behavior of a system of agents each following relatively simple ›scripts‹. The exponentially increasing complexity of the training systems, gradually assembled from reusable contractor components, which only allows for intuitive predictability, appears to be sufficient to legitimize the mapping of culture onto a technological setup in operational terms, i.e. through repeated, conditioned use of the respective tools.

For AI computation in both military training and digital games, MOUT situations are defined according to template topographies like »techniques for a hallway, a stair well« as the training documentation describes it and other recurring spatial elements. (McDonald 2003, 25) The functional segmentation of an integral environment into ›patterns‹ complies with the notion of identifying template situations for which to write reusable code in digital game AI and programming in general. The seminal book *A Pattern Language* by Christopher Alexander and colleagues represents a piece of conceptual groundwork in that direction which was derived from architecture but later informed computer science and digital game programming in particular. (For extensive excerpts from the book, particularly patterns related to town and community design, cf. e.g. http://downlode.org/etext/patterns/)

These aspects of MOUT AI are aimed at complexity reduction and closely resemble strategies used to render terrorism conceptually manageable in digital games; observing these patterns rather than 'hard-coded' visual or narrative topoi in selected games can thus yield valuable insights into the effects of programmable media on popular conceptualization of terrorism. For instance, the RTS game COMMAND & CONQUER: GENERALS (EA Pacific, 2003) combines simulacra of Afghan, Iraqi and generic Oriental icons of terrorism, implementing playable units like an ›angry mob‹, suicide bombers simply labeled as ›terrorists‹ in the game's nomenclature, chemical weapons and a ›SCUD launcher‹, thereby creating a computable gameplay ecology resulting in a spectrum of emergent micronarratives of terrorist behavior with a much higher degree of perceived authenticity than traditional cinematographic or literary forms. The plausibility of the algorithms, rather than the reliability of information sources or the familiarity of narrative conventions, has become the key criterion for representations of terrorism.

Thus, just as earlier games like chess shaped ›best practices‹ in contemporary military strategies, programmable media define the current strategic imaginary. **◂2** The goal of the following paragraph will be to broaden the recurring notion of ludicity beyond dedicated games used for military purposes.

Ludic Application within Programmable Media Developments

»Computer-mediated communication« (as e.g. in Daisley, 1994) and particularly programmable media objects will, for the purpose of this argument, be conceived of as inherently ludic. While this article is concerned with recent phenomena, this certainly applies as well to older, analogue media technologies which can be understood as ›programmable‹ such as musical dice games and also military applications. Concerning digital games, this implies a definitorial shift of focus, from considering them as essentially ›games played on a screen‹ (cf. the early popularity of the German term ›Bildschirmspiel‹) towards ›programmed applications foregrounding and maximizing their inherent ludicity‹.

This phenomenon has been tentatively approached from several directions. For instance, Martin Lister acknowledged the playfulness of programming itself, based on the premise that in the early days of digital games, programming even simple languages like BASIC was a commonplace concurrent practice when playing games. (cf. Lister 2003, 265). Playfulness is also one of the key characteristics of the ›hacker‹ archetype in fictional works like Lawrence Lasker and Walter F. Parks's *Wargames* or cyberpunk novels like William Gibson's *Neuromancer* and Neil Stephenson's *Snow Crash*. Moreover, as Claus Pias briefly notes, William Higinbotham's *Tennis for Two* was already a playful repurposing of programmable hardware. Even the logic of the ›sequel‹, a modified version which was released the following year, can be conceived of as the product of a playful over-stretching of the initial semantics of tennis devised to make sense of the abstract point and bars displayed on the oscilloscope; adding a modifiable gravity constant was the technologically easiest way of producing emergent alterations of the ›implied game‹ and was consequently re-semanticized as playing tennis on the moon or Jupiter. (cf. Pias 2004, 5)

An example of inherent ludicity in military contexts are agent-based simulation environments like PS-I (Political Science: Identity), used e.g. by political scientist Ian Lustick for modeling social transformations in a *Virtual Pakistan*. **◂3**

The open-source PS-I software is essentially a rather complex cellular automaton, used in the project to represent the spatial distribution of ethnic identities in Pakistan on a grid consisting of colored squares. Given the scope of this article, I can only exemplarily offer a number of vantage points, i.e. meaningful restrictions of the program, to analyze the formative effects of technology usage both on the respective concept of culture and on the perceived affinity towards terrorism in particular.

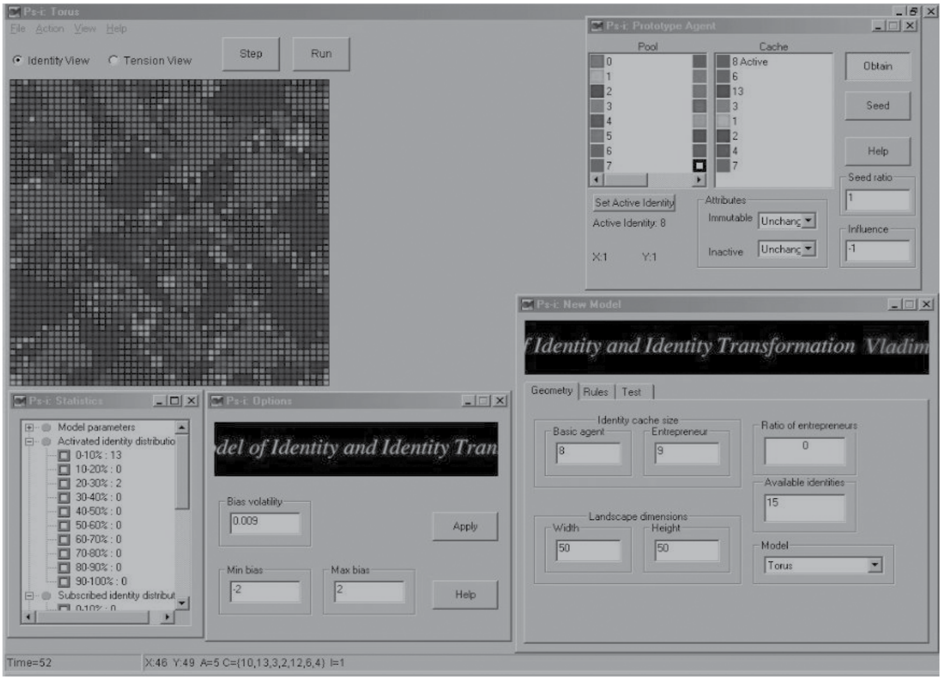


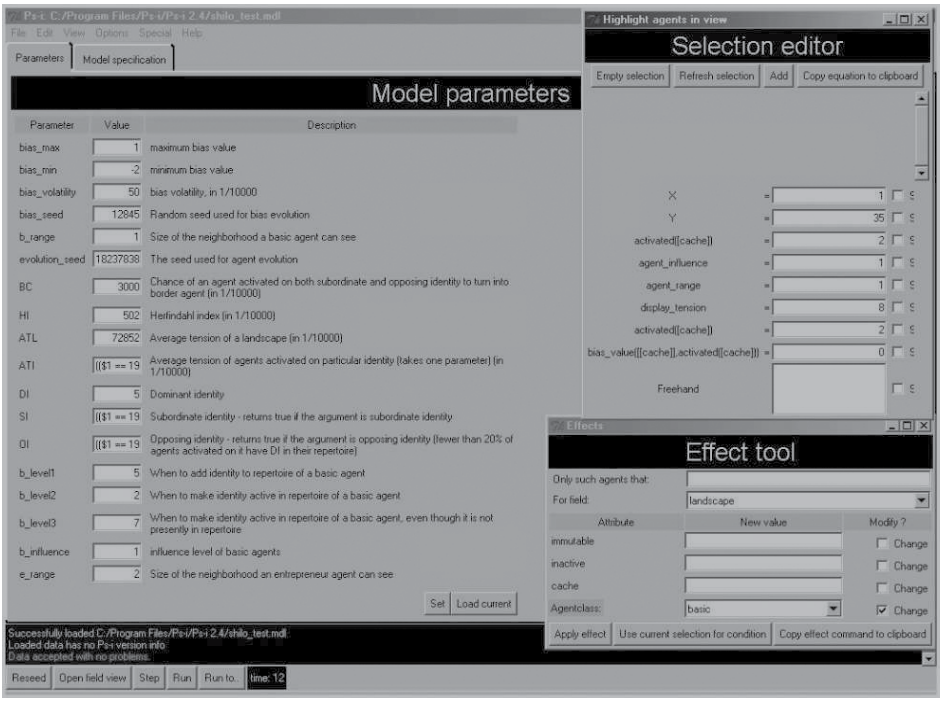
Abb. 1-2 (opposite page): Screenshot of the PS-I software(Political Science: Identity), used for modeling social transformations in a Virtual Pakistan5.

First and foremost, the quasi-agent-based simulation requires a set of discrete ›identities‹; any cell representing a group of people has one ›activated‹ identity but can have multiple latent, i.e. ›subscribed‹ affiliations (Lustick 2003, 6). Apart from ethnic and religious identities, social and economic status indicators are also available.

Another aspect is the quasi-spatiality of the model which is particularly designed to model local identity transformations, i.e. effects on adjacent squares. Placing four »broadcast agents« that can affect only members of particular identities assumed to be »attuned to politics« is a first but obviously still rudimentary step to overcome this limitation (Lustick 2003, 21).

Most conspicuously, the model draws heavily on the plausibility of averaging, a principle largely derived from and plausibilized by programmable media, not least digital games. Unavoidable inaccuracies are to be primarily compensated by iterated runs, randomizing the »distribution of ›biases‹« and the variables of the identity-switching algorithm (Lustick 2003, 7).

The conceptual adequateness of apparently overlapping politico-institutional and simulation categories, most notably the four major provinces constituting *Virtual Pakistan* which roughly match the actual formal political situation, is uncritically implied. The contingencies of the simulation and the clearly, even (within the confines of the software) ›ontologically‹ differentiated regions, in reverse, stabilize the perception of the respective geographic regions in Pakistan as a given, occluding the numerous political and social complexities which are masked by the institutionalized regional constellation. According to the document, »characteristic clusters of latent identities« (Lustick 2003, 11) and the representation of Pakistani black economy by a high visibility of the »criminal/smuggler identity« (ebd., 22) were criteria for the initial configuration; i.e., an intuitive representation of familiar factoids serves as the criterion for operational authenticity. Concrete political models like the vision of Pakistan as a country for Muslims rather than Islam formulated by Ali Jinnah (ebd., 15) also fed into this initial configuration and were conceptually ›homogenized‹ by being translated into code and variables.
A first, seemingly trivial indictor of the ludic potential in the PS-I framework and of the semiotic conditioning of its specific representational mode is the



simple fact that the project homepage playfully takes up the same colored squares used to indicate the system behavior. ◂**4**

Educated ›playing around‹ with the simulation, e.g. to determine the »baseline« settings (ebd., 19) used for normalizing the findings, is an important aspect of the actual usage of the tool. ◂**5** More importantly however, the interpretation of the results is necessarily playful to a certain degree, representing ›jigsaw puzzle pieces‹ that need to be meaningfully reassembled. For instance, a threshold was set for public tension in the vicinity of »nuclear stockpiles« (based on real-world knowledge); if the tension level exceeded a critical value, a »nuclear event« would be triggered, providing a new category of analysis. (ebd., 27) The resulting finding that »futures«, i.e. iterated runs, of *Virtual Pakistan* with a nuclear event turned out less successful on average compared to those without then coincides again with common sense expectations. (ebd, 27)

Again, this type of technology has been and is concurrently being developed for use in digital games like the very ambitious REPUBLIC – THE REVOLUTION (Elixir Studios, 2003). The distributed AI in this game, also building on hundreds of agents implemented as finite-state machines, measures a NPC's stance towards the »government, religion, political philosophy, morality, economics, violence, ethnic tolerance, and international relations« (cf. Mayer/Hassabis 2001/02, S. 37f.) which, as the developer diary reveals, also turned out to produce emergent behavior which transcends even expectations based on a profound knowledge of the program. Players would experiment with these dispositions of their inhabitants to earn three ›resources‹ - fear, money, and influence (ebd., 37). While this might seem cynical for an actual simulation, and clearly contains politically motivated bias on the behalf of the game and AI designers, the structural congruence with tools like *Virtual Pakistan*, most notably the translation into a handful of key variables and rules, is striking.

One of the most important but maybe most overlooked aspects of the simulation, although Lustick is rather an analyst than a political consultant, is the fact that the tool is freely downloadable ›to play with‹, representing the type of ›distributed‹, decentralized strategies that a political agenda based on OOP-based techniques of analysis and implementation would call for.

My argument thus assumes an inherent momentum of programmable media technologies used both in civilian and military contexts to propagate a mathematical understanding of terrorist or any complex social behavior. In this respect, it is important to acknowledge the conceptual overlaps with older, colonial tools of governance like the census, the impact of which collective sentiments like nationalism has been canonically outlined by Benedict Anderson

(cf. Anderson 1991, 164ff.). Anderson notes that in the course of colonial governance (in South-East Asia), the identity categories of the census, seamlessly mappable to the types of identities used in *Virtual Pakistan*, gradually shifted from religious classification to racial criteria. Colonial government can only now, in retrospect, be interpreted in these terms, yet the criteria for this ex-post historical perspective can, on a smaller timescale, be applied to documented applications of models like *Virtual Pakistan* for actual politico-military decision-making. This could yield a more solid perspective on the effect of these media technologies on their usage, similar to the effect of the census not only on the governed but also on the governing factions. An example could be the use of the tool *PowerScene*, ◂**6** half tactical mapping program, half flight simulator, which has been used both for military planning and for determining an appropriate consensus in the Dayton Peace Accords following the conflict in the Balkans in the mid-1990s. At least a rudimentary awareness of the signifying potential of the technology is indicated in a report which states that the quality and especially consistency of the map data in *PowerScene*, enabled by using a unified data structure for all map images, were used strategically to intimidate the Serbian political leaders and discourage further aggression by relatively suggesting the ›perfect‹ transparency of the enemy territory and forces (cf. Johnson 1999, 3).
Anderson's insightful analysis of the census can, by inference, provide more viewpoints to look at the current use of social simulation tools. One of the most important effects for colonial governments was not only to obtain a normalized overview of the population but, inversely, the homogenizing potential to produce a population fitting the census. By analogy, programmable media with similar characteristics can have an equally homogenizing effect which is especially relevant in multi-national military operations and e.g. in U.S. training of Iraqi troops where conventional »top to bottom« approaches seem to fail. ◂**7**

Confounding Explanatory Systems through the Proxy of Program Code

Algorithms for modeling social systems (cf. e.g. CNS 2006) are a hotly debated topic and theoretical role models for analyzing terrorist activities as social systems are increasingly derived from other explanatory domains like physics. (For a representative recent example cf. e.g. Clauset/Young 2005) Therefore, it is worthwhile to examine how program code and especially the structural properties of programming languages encourage the ›transcoding‹ of terrorism as a socio-political phenomenon into other explanatory systems such as biology and physics. While a comprehensive overview of program code in general and the OOP paradigm in particular is not feasible within this text, some key elements are the definition and nesting of generic methods and object classes that can process variables in a prestructured form, the general modularity of program code components given consistent method and variable declarations, and particular OOP elements like encapsulation and inheritance. **◂8**

Interestingly and often inadvertently, this has been standard practice in digital games programming for decades. Chris Crawford's EXCALIBUR (Atari Program Exchange, 1983) aptly illustrates this principle with its routines for calculating the dynamic relationships between the Knights of the Round Table and the player character, King Arthur (Crawford 2003, 272f.). The closeness of a knight towards Arthur or another knight is indicated by the relative position of their shield symbols in a 2-dimensional field, with Arthur immovably occupying the center of the screen. Thus, the resulting model of social cohesion algorithmically reflects the laws of magnetism, pushing and pulling the board pieces into a significant constellation with very few simple behavioral rules.

Probably the main reason for translating social complexity into models derived from natural sciences is the feasibility of algorithmically expressing these established rule systems. Yet, a semiotic close reading of this process could uncover a number of built-in contingencies like the naturalization of particular explanatory gestures which also permeates language use and, through that, pre-structures thinking about an issue like terrorism. For example, using biological models of computing terrorist activity coincides with the semantics of the ›war on terrorism‹ which attempts to liken it associatively to a campaign against an unquestionably negative ›natural anomaly‹ like the ›wars‹ on cancer or against climate pollution; this issue was e.g. convincingly explored by Susan Sontag in an article in the *New York Times* in 2002, yet it would go beyond the scope of this article to recapitulate the argument in detail. **◂9**

Accordingly, mathematical game theory is usually proposed as a way of modelling ›information warfare‹ strategies (cf. e.g. Jormakka/ Mölsä 2005). Just as in the case of complexity reduction based on the necessity of algorithmically expressing a conflict situation, e.g. in a digital war game or training simulation, the mathematicization of the information warfare has built-in implications both on the understanding of the conflict and even on actual policies drawing on these models. For instance, due to game-theoretical conventions, these models presuppose a binary opposition between »pure« and »mixed« strategies, the latter being represented by a probability distribution (ebd., 13). Due to their massive, increasing usage since the early 1950s, models of calculation like this can be plausibly assumed to shape and constrict the politico-military imaginary. Furthermore, the article by Jormakka and Mölsä mathematically ›proves‹ the rationality of governments employing a »bold« playing strategy when negotiating with terrorists, showing that the terrorists' net gain will eventually reach a critically low point (ebd., 16). It thereby mathematically validates a currently popular notion in foreign policies by employing a particular ›algorithm‹, in this case the Nash equilibrium points being derived from the respective payoff functions, and its conceptual obfuscation to conceal the fact that the basic premise in this case was an arbitrarily chosen payoff matrix. The fact that the theoretical outcome is legitimized by coinciding with personal experience in recent years (ebd., 17) completes the circular argument. As a side effect, the particular strategy is fixated in political discourse by being mapped onto a discrete calculation method.

Hence, a key side-effect of terrorism modeling in the age of programmable media is the belief in the asymptotic computability of complex socio-cultural phenomena it produces. This idea, combined with the confounding of explanatory systems outlined above, can be applied to more recent examples which leads to the hypothesis that concurrent trends in other computer science disciplines like graphics algorithm programming are also implicitly fed into the convergent use of programmable media in both military and civilian contexts.

For instance, a hot topic discussed at *Siggraph* 2006, one of the leading annual conferences on computer graphics, was the dynamics of crowds; one characteristic approach proposes a departure from agent-based models of crowd behavior, i.e. calculating each person's behavior in a crowd, which are a currently popular method used both for digital games and e.g. computer graphics in films, towards continuum dynamics (cf. Treuille et al. 2006). Continuum mechanics, in turn, are the paradigmatic field of study applied e.g. in modeling a fluid behavior composed of continuous particles or molecules. Thus, again, modeling algorithms for a natural phenomenon are being transferred to the study of social systems; it is probably safe to assume that the fact that a house evacuation was chosen as a case study for the demonstration video was not incidental. **◂10** Unlike the initial example *Excalibur*, however, this case hints at the particular dynamics and mutual shaping of the converging technological development for digital games and military simulation purposes. For instance, the need for realistic crowd behavior in current military training overlaps with recent game projects like ASSASSIN'S CREED (Ubisoft Montreal, Q4 2007) and TOM CLANCY'S SPLINTER CELL: CONVICTION (Ubisoft Montreal, TBA 2007) designed to showcase the potential of the so-called ›next-generation‹ console hardware.

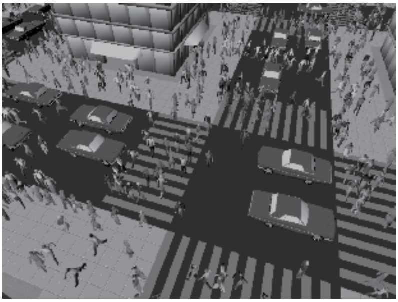


Abb. 3-4: Scrennshots of EXCALIBUR (Atari Program Exchange, 1983) and of the demonstration video for the CONTINUUM CROWDS model

The simultaneous development of these two high-profile titles by the same company, Ubisoft Montreal, strongly hints at the exchange of code or at least knowledge and, thus, at the aim for creating a modular, reusable piece of code that might be transplanted into other programmable media contexts.

Interestingly, the demonstration video for the *Continuum Crowds* model also exemplifies the ›inherent ludicity‹ hypothesis by closing with a UFO flying through a street scene, demonstrating the emergent behavior and priority shifting of crowds of AI agents in a playful fashion while ›debugging‹ the application, i.e. strategically (over)straining its rule system as is common in a situation characterized as ›ludus‹ according to Caillois.

With regard to terrorism, when the enemy is interpreted according to computability criteria, the resulting strategies will likely follow the same logic. An early model for estimating required naval force levels (cf. Hurley 1995) illustrates this tendency. Hurley's model is based on the paradigmatic unit of Excel spreadsheets and thus carries the software's built-in bias or contingencies. One effect of the model is the binary distinction between peacetime and conflict scenarios, shifting the reference variable accordingly (ebd.,8). Another interesting feature of the model is its intended compatibility with other models like a simple cost model (ebd.) which indicates that approaches based on standardized software already predated the currently expanding notion of modularization.

More importantly, the use of standardized software can be assumed to effectuate epistemological overlaps with the sphere of civilian ›work‹ and thus fundamentally re-informs the status of the military in society. The recently decreed shift towards open source in a memorandum by the Department of the Navy ◂11 underlines this hypothesis.

Further Case Studies

A case study to demonstrate the usefulness of the ›program code‹ model to comparatively analyze seemingly heterogeneous ›strategies‹ is the AI-based simulation DEFACTO devised for fire-fighter training at the University of Southern California (USC) (cf. e.g. Piquepaille 2007).
Formerly, to train firefighters for different types of emergencies, an expert team would create fictional disaster scenarios from their own experience and act as a responsive ›environment‹ by producing ›input‹ (like bulletins etc.) to mimic an actual case of emergency. The goal of DEFACTO is to hand over this process to an agent-based AI which can be conceived of as essentially a dedicated ›storytelling‹ algorithm for generating interactive emergency scenarios, quite similar to reusable pieces of code used for randomized scenario generation in digital games like WESTFRONT (Talon Soft, 1998), SID MEIER'S ANTIETAM! (Firaxis Games, 1999) or WINGS OVER EUROPE: COLD WAR GONE HOT (Third Wire, 2006).
While it is not explicitly mentioned in the above-mentioned project description, the experience with the terrorist attacks of September 11, 2001, channeled by media representations such as Nicholas Cage's iconic impersonation of a firefighter at ›Ground Zero‹, inextricably linked firefighting to the issue of preparing for perceived terrorist threats and DEFACTO needs to be regarded in that context. The initial example in the technical working paper is the series of hurricanes that hit the south of the United States in 2005 and reaffirmed the call for a solid disaster prevention system (cf. Schurr et al. 2006). Yet, the research project, which appears to have a dedicated ›civilian‹ agenda, is funded by the Center for Risk and Economic Analysis of Terrorism Events (CREATE), the first university center directly supported by the U.S. Department of Homeland Security. This type of relation represents another important repercussion of the confounding of civilian-military boundaries effectuated by the convergence of programmable media technologies in both domains. At the very least, the › dual use‹ of tools like DEFACTO inherently plausibilizes the conceptual linkage of »natural and man-made« (ebd., 1) disasters like terrorism legitimating their theorization in similar terms.
Firstly, the readiness to supplant the experience of experts with so-called ›expert systems‹ is an interesting indicator in its own right which speaks of characteristically human features like ›experience‹ becoming less relevant. Second, the widespread application of this system leads to the collective imaginary of disaster scenarios being shaped by the programmable medium which, according to the previous assumption, can be thought of as inherently ludic. Third

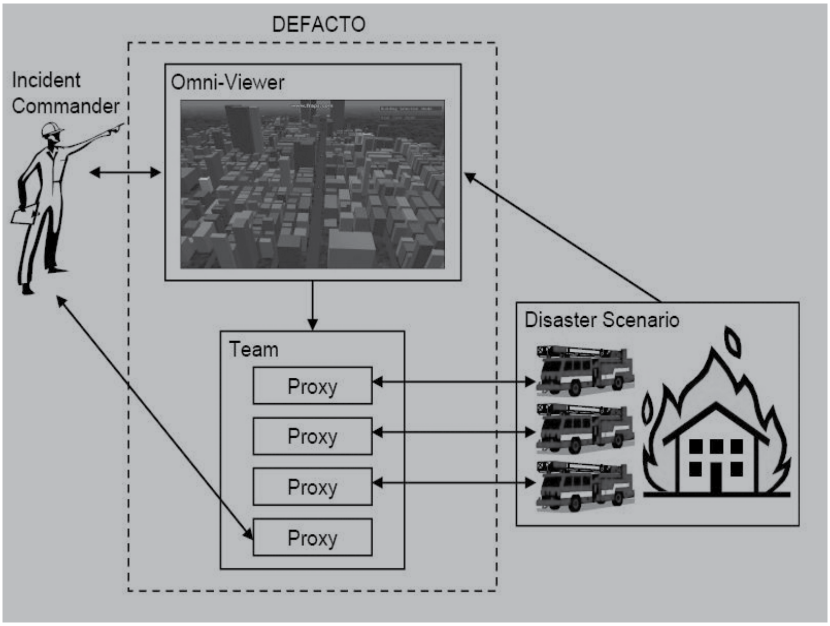
and most importantly, the program is designed to train firefighters in »[delegating] some power to the AI software agents «i.e. allowing »humans and agents to work together in teams«. ◂12 This requires firefighters to adopt the logic behind specific AI routines at least on an operational level by integrating them into their work routines – and subsequently applying this logic to real-world situations as the software is also designed for actual deployed applications. One concrete effect of this ›delegation system‹, based on the idea of automatically adjustable autonomy of the software agents, is that it requires an absolute concept of hierarchies to determine algorithmically how to distribute responsibilities and autonomy; if no qualified decision is reached, all tasks are ultimately handed to the ›incident officer‹ as the highest-ranking and, according to the system, universally most capable ›agent‹. Furthermore, while the system is internally absolutely deterministic, its implications are so complex that fine-tuning can only be performed on the basis of observing and hermeneutically assessing it in default scenarios. (Schurr et al. 2006, 3) This kind of ›AI interaction‹ is again iteratively ›rehearsed‹ by players of (not just military-themed) digital games. A prominent upcoming example is the aforementioned Splinter Cell: Conviction which aims at mimicking cinematic conventions by having the player character automatically ›choose‹ the most appropriate move from a repertoire of animation cycles upon attacking an enemy depending on the situation, e.g. the relative position towards the enemy and other variables (cf. EDGE (*German Version*) 7/8 2007, 65). This is achieved by AI routines taken over from enemy behavior scripts which semi-automatically co-direct the outcome of a situation and, simultaneously, ›condition‹ players to factor their iteratively refined knowledge of how this system works into their playing style.

A broader look at recent patents tagged as pertaining to topics like ›modeling‹ and ›terrorism‹ complements and ›colorizes‹ the existing picture. For instance, patent No. US 6,795,795 B2, filed in 2004, describes the probabilistic mapping of a building according to the likelihood of chemical, biological or other agents as the result of a terrorist attack. (cf. Kreichauf 2004) The building in question will be dissected into floors and »cubes« (ebd., 1) and equipped with sensors in each cube, constantly relaying data to a central processing unit. On a display, the probability of agents in a cube will be displayed by shading or coloring the respective cells, (ebd., 3) similar to the representational mode used in the PS-I simulation of social transformation in Pakistan.

Again, the semiotic implications of tools like this are not discussed; color-coding the probability of a terrorist attack, depending on seemingly peripheral aspects like the contingent selection of colors, can have very tangible practical consequences, leading to an iterative cycle in which the tool generates the reasons for its own existence. Yet again, similar algorithms, e.g. the discrete zoning of an environment, are also being used in digital games; probabilistic mapping and especially finite state machines are recurring topics in AI programming. For instance, Alexander Nareyek briefly hints at the potential of probabilistic networks for in-game AI, although not primarily for character control but for pre-computing graphics based on educated assumptions of the player's next move (cf. Nareyek 2004, 3). Thus, the functional ›perception‹ of an environment similar to AI routines is designed to be translated into a tool for human security personnel in large buildings. Epistemologically, this is a big step towards the ideal in military training (and games) of soldiers to ›fuse‹ with the programmable framework they operate.

Patent No. 6,574,561 from June 2003 proposes a geographic emergency management system and exemplifies yet another representative effect of programmable media technologies, the physical extension of OOP structures, even more clearly than the previous example. (cf. Alexander et al. 2001) The system essentially consists of a number of GPS-capable receivers which again automatical-

Abb. 5: Process scheme of the AI-based simulation DEFACTO devised for fire-fighter training at the University of Southern California



ly transmit data to a central processing unit combining all heterogeneous input in a geographic database. In this sense, it is a physical manifestation of the programming principle of having event handlers autonomously registering a particular form of input like e.g. the player passing an invisible trigger object in a game which is then collected and interpreted by a central script, e.g. an AI loop, and assembled into a more or less homogeneous picture. This example might serve as a role model for identifying principles of program code translating into real-world strategies as in the aforementioned case of the Stryker brigade.

Since patent databases are regularly consulted both by companies and inventors, a comparative look at patents related to a particular technique like terrorism modelling read against concurrent notions in politico-military discourse can yield insights into and patterns of the peculiar dynamics of the collective imaginary as shaped by programmable technologies which can and should plausibly be understood as media.

Conclusion

In a geo-political constellation shaped by the specter of terrorism and its structural properties, technologies more than ever occupy a central position in delivering a promise of security. A key report compiled by the National Academies' National Research Council, commissioned and prepared immediately after September 11, 2001, accordingly highlighted areas of weaknesses against asymmetric warfare and sketched the role of science and technologies both in preventing attacks and attenuating their impact. **◂13** cf. To pointedly conclude this article, contemporary forms of terrorism, at least according to scholarly (and public) conceptions shaped not least by the pervasiveness of digital games, can be argued to represent and thereby impose principles of object-oriented programming onto the public understanding of warfare, legitimating their use in search for counter-measures.

According to a comprehensive report commissioned by the Institute for Security Technology Studies (ISTS) from January 2001, terrorist acts using bio-weapons and biological warfare strategies dominated the political agenda. (cf. Joseph/ Lucey 2001, 103-105) One particularly relevant project sketched in the report was the ›infrastructure web‹, an attempt to extend the structural properties of the internet to include the protection of »critical national infrastructures« (Joseph/ Lucey 2001, 198) in the United States. **◂14** The feature list illustrates how this, already before the formative experience of 9/11, effectively entails applying the logic of OOP to include physical objects as exemplified above; the projected system was described as »decentralized, asynchronous«, »searchable and self-organizing« as well as »allow[ing] for multiple, redundant communication paths between entities« (Joseph/ Lucey 2001, 199), i.e. ›objects‹ which in this context could mean anything from a singular sensor to a whole building or site.

The aforementioned report on the use of technologies in countering terrorism contains a similar proposition, an adaptive electric-power grid which also ideally possesses self-regulating functionality, automatically adapting to malfunctions or attacks through quasi-OOP properties of the individual nodes in the grid. Interestingly, it is mentioned in passing along with other propositions referring to actual information technologies.

This case also recapitulates surprisingly from a pre-9/11 perspective the use of alternative explanatory models like biological semantics and structural metaphors, describing e.g. the phases in the timeline of a particular hacking technique as »[mutations]« of the original phenomenon, (ebd.,199) indicating the structural congruence between the programmable media technology (in this case Distributed Denial of Service attacks) being continually reprogrammed and changes in biological evolution. Later, the repercussions of infrastructure vulnerabilities are conceptualized by proposing quantitative models of »infrastructure epidemiology«, (ebd., 201) yet again stabilizing the perception of terrorist attacks not as asymmetrical warfare but as a disease. A few years later, the elusive concept of the ›information warfare‹ was tentatively made ›compatible‹ with public discourse by using very similar biological metaphors and concepts e.g. taken from entomology (cf. e.g. Kopp 2000) which, not least due to the experience with digital games as elaborated above, were already plausibilized and workable. The general model of the ›information warfare‹ can be implicitly understood as the ideal type of a computer program, not least since the Borden-Kopp model which outlined it was already conceived for mathematical (and, thereby, algorithmic) supportability in 2001 (ebd.,1). In this sense, the plausibility of the entomological role models used to formulate and illustrate the four basic strategies of information warfare (i.e. denial of information, mimicry, disruption and subversion) even proved to be sustainable enough for them to function as ›reusable code‹ which could later be translated into military practices and micro-strategies.

The processes sketched in this article and the convergence of programmable media use in civilian and military contexts are continually intensifying. As a tentative outlook, online-capable digital games like America's Army which encourage large-scale and monitored iterative replaying can be understood as technologically ›cross-linking‹ players, not only during the act of ›screen-playing‹ but in their entire media usage, into a vast ›distributed system‹ modeled after the structure of the program code they manipulate. This process closely resembles principles of earlier distributed computing endeavors such as the SETI@Home project, except that both the technological and epistemological demarcation lines are not as clearly drawn but playfully pushed back and forth. However, as the ephemeral but still influential archetype of the hacker illustrates, the potential dangers for the socio-technological apparatus outlined in this article can and will equally be reversed and challenged by the very same technologies producing their own ›antidote‹.

Anmerkungen

01▸ One prominent example of how the phrase is stabilized in public discourse is the official website Defend America55 (cf. http://www.defendamerica.mil/) where the phrase is featured in the subheading.

02▸ For an inquiry into the formative effects of chess, including an example of how the role model of the game is still present in contemporary strategy, cf. e.g. http://www.guardian.co.uk/life/feature/story/0,13026,1161128,00.html.

03▸ The project is extensively documented with illustrations of the graphical user interface (GUI) in (Lustick 2003).

04▸ The URL of the website in question is cf. http://web.archive.org/web/20050827083705/www.psych.upenn.edu/sacsec/abir/.

05▸ A news bulletin about the project at the University of Pennsylvania illustrates the quasi-ludic approach to varying starting variables like the 'perception range' of cells; cf. http://www.sas.upenn.edu/home/news/lustick.html.

06▸ For a useful overview of Powerscene55 and its usage history, cf.: http://www.tec.army.mil/td/tvd/survey/PowerScene_aka_CVPS.html.

07▸ An example of common organizational problems encountered can be found e.g. at: cf. http://www.military-training-technology.com/article.cfm?DocID=1971.

08▸ Since OOP is usually discussed in the context of a particular programming language, comprehensive works on the topic are hard to find. A useful collection of introductory reads can be found at: http://www.oopweb.com/.

09▸ The full text is available on-line at: http://humanities.psydeshow.org/political/sontag-2.htm.

10▸ The video is available on-line at: http://grail.cs.washington.edu/projects/continuum-crowds/movs/continuum-crowds-divx.avi.

11▸ The full memorandum text can be found on-line at: http://oss-institute.org/Navy/DONCIO_OSS_User_Guidance.pdf.

12▸ The full project documentation is available on-line at: http://teamcore.usc.edu/schurr/research.shtml.

13▸ The report is archived on-line at: http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=s10415.

14▸ The project was consequently pursued further after September 11, 2001, as documented e.g. in: http://www.ists.dartmouth.edu/library/spi0602.pdf.

Bibliografie

Alexander, John Franklin et al. (2003): Emergency Management System. U.S. Patent No. 6574561. (http://www.google.de/patents?id=IlF8AAAAEBAJ (zuletzt einges. 17.09.2007).

Anderson, Benedict (1991): Imagined Communities. Reflections on the Origin and Spread of Nationalism. London/New York: Verso.

Center for Nonproliferation Studies (CNS) (2006): Literature Review of Existing Terrorist Behavior Modeling. http://cns.miis.edu/pubs/reports/terror_lit.pdf (zuletzt einges. 17.09.2007).

Pias, Claus (2004): Die Pflichten des Spielers. In: Martin Warnke / Georg C. Tholen/ Wolfgang Coy (Hg.): Hyperkult II. Zur Ortsbestimmung analoger und digitaler Medien. Bielefeld: (transcript), S. 313-342 (hier zit. nach: http://www.uni-essen.de/~bj0063/texte/pflichten.pdf (zuletzt einges. 17.09.2007).

Clauset, Aaron,/ Young, Maxwell (2005): Scale Invariance in Global Terrorism. http://arxiv.org/abs/physics/0502014 (zuletzt einges. 17.09.2007).

Corsi, Jerome R. (1981): Terrorism as a Desperate Game. Fear, Bargaining, and Communication in the Terrorist Event. In: Journal of Conflict Resolution 25:1, S. 47-85.

Crawford, Chris (2003): On Game Design. Indianapolis, Ind. : New Riders

Daisley, Margaret (1994): The Game of Literacy: The Meaning of Play in Computer-Mediated Communication. In: Computers and Composition 11:2, S. 107-119.

Friedmann, Ted (1999) The Semiotics of SimCity. In: First Monday 4:4. http://www.firstmonday.org/issues/issue4_4/friedman/index.html (zuletzt einges. 17.09.2007).

Grammont, Steve (2007): Combat Mission: Shock Force Q&A: Simulating Modern War. http://www.gamespot.com/pc/strategy/combatmissionshockforce/news.html?sid=6165874&mode=previews&print=1 (zuletzt einges. 17.09.2007).

Hurley, William J. (1995): Model For Estimating Naval Force Levels (IDA Document D-1570). http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA291728 (zuletzt einges. 17.09.2007).

Johnson, Richard G. (1999): Negotiation the Daytona Peace Accords Through Digital Maps. In: United States Institute of Peace, Virtual Diplomacy Report. http://www.iapad.org/publications/ppgis/Negotiating_the_Dayton_Peace_Accords_through_Digital_Maps.pdf (zuletzt einges. 17.09.2007).

Jormakka, Jorma/ Mölsä, Jarmo (2005): Modelling Information Warfare as a Game. In: Journal of Information Warfare. 4:2, S. 12-25.

Kopp, Carlo (2000): A Fundamental Paradigm of Infowar. In: Air Power Australia (APA). http://www.ausairpower.net/OSR-0200.html (zuletzt einges. 17.09.2007).

Kreichauf, Ruth D. (2004): Probabilistic Map for a Building. U.S. Patent No. 6795795. http://www.google.de/patents?id=UJASAAAAEBAJ (zuletzt einges.:17.09.2007).

Lister, Martin et al. (Hg.) (2003): New Media: A Critical Introduction. Oxford: Routledge

Lustick, Ian (2003): Virtual Pakistan and Its Futures: An Exercise in the Deployment of Constructivist Theory. http://www.psych.upenn.edu/sacsec/abir/_private/publications/VirtualPakistan_CAEG.doc (zuletzt einges. 17.09.2007).

Mayer, Jonathan / Hassabis, Demis (2001/02): The Elixir Diaries. Originally published periodically in EDGE Magazine. http://republic.strategyplanet.gamespy.com/diaries.shtml (zuletzt einges. 17.09.2007).

McDonald, Grant (2003): MOUT Training. The Increasing Need. In: Military Training & Simulation News 5:6, S. 23-28.

Nareyek, Alexander (2004): AI in Computer Games. In: QUEUE, February 2004

Piquepaille, Roland (2007): Using AI to Train Firefighters. ZDNet Blogs: Emerging Technology Trends, 6 Jun., 2007. http://blogs.zdnet.com/emergingtech/?p=596 (zuletzt einges. 17.09.2007).

Rosen, Joseph/ Lucey, Charles (Hg.) (2001): Emerging Technologies: Recommendations for Counter-Terrorism. Institute for Security Technology Studies January 2001. http://www.dartmouth.edu/~engs05/md/whitepapers/Emerging_Tech/ETech.pdf (zuletzt einges. 17.09.2007).

Schurr, Nathan et al. (2006): Using Multiagent Teams to Improve the Training of Incident Commanders. Proceedings of the Industry Track of the Fifth International Joint Conference on Autonomous Agents and Multiagent Systems. http://teamcore.usc.edu/schurr/papers/AAMAS06IND.pdf (zuletzt einges. 17.09.2007).

Treuille, Adrien et al. (2006): Continuum Crowds. ACM Transactions on Graphics 25:3. http://grail.cs.washington.edu/projects/continuum-crowds/ (zuletzt einges. 17.09.2007).

Gameography

Assassin´s Creed, Ubisoft Montreal, Q4 2007.

Combat Mission: Shock Force, Big Time Software, 2007.

Comand & Conquer: Generals, EA Pacific, 2003.

Excalibur, Atari Program Exchange, 1983.

Fugitive Hunter: War on Terror, Black Ops Entertainment, 2003.

Full Spectrum Warrior, Pandemic Studios, 2004.

Republic – The Revolution, Elixir Studios, 2003.

Sid Meier's Antietam!, Firaxis Games, 1999.

Tom Clancy´s Splinter Cell: Conviction, Ubisoft Montreal, TBA 2008.

War on Terror, Digital Reality, 2006.

Westfront, Talon Soft, 1998.

Wings over Europe: Cold War Gone Hot, Third Wire, 2006.