Smart Cities: interacţiune, adaptare şi auto-organizare

MD Emil VELCEA
CCISO

velceaemil@yahoo.com

Rezumat:

Tendința accelerării ritmului de dezvoltare socială este des menționată în studii de specialitate și prezentări în mass media; constatăm utilizarea frecventă a conceptului „Societate a cunoașterii". *Concepte perimate (axate pe producția valorilor materiale), precum* „Societatea industrială" *și* „Societatea Agrară", *sunt înlocuite, astfel, de o* „Societate a cunoașterii" *în care, recunoscând și utilizând puterea informației în procesul de modelare a deciziilor, întâmpinăm și percepem – diferit și avizat – provocări viitoare, precum:* accelerarea ritmului inovărilor noilor produse/serviciilor, proliferarea acestora, sporirea importanţei autorităţilor publice locale, acutizarea problemelor ecologice, *etc.*

În acest context, conceptul „smart city" *și tehnologiile* „smart" *pătrund, din ce în ce mai mult, în cunoașterea generală, noi (cetățenii) fiind martori/ observatori ai inițiativelor ce vizează implementarea unor proiecte al căror specific se aliniază perfect provocărilor viitorului (de ex. asigurând monitorizarea și optimizarea consumului resurselor disponibile, precum și asigurarea unui nivel ridicat de securitate și confort urban).*

În prezentarea „orașului inteligent" *nu am dorit re/definirea acestui concept (varietatea tehnologiilor care au fost implementate, sub această etichetă, oferind, totuși, posibilitatea exprimării unor diverse, puncte de vedere); am adresat însă – într-o formă, sper, coerentă, integrată – concepte precum:* „ecosistemul tehnologic", „orașul inteligent", „adaptarea", „autoorganizarea" „infrastructuri critice", „rezilienţa".

Cuvinte cheie: *ecosistem cibernetic, smart city/oraș inteligent, Sisteme Adaptive Complexe (CAS).*

Cum va arăta viitorul ? Care vor fi cele mai presante probleme în agenda dezvoltării urbane, în următorii 20-30 de ani ?

Este greu de prezis, însă analiza tendinţelor actuale ne oferă indicii concludente privind potenţialul (semnificativ) de dezvoltare al „*oraşelor inteligente*[1]", relaţionarea unor concepte precum „*Integrarea*" şi „*Interconectarea*" (de exemplu, a tehnologiilor) fiind deseori menţionată, în studiile de specialitate şi mass media.

[1] Corespunzând expresiei din limba engleză « *smart city* ».

Alăturarea acestor concepte, celui care identifică/prezintă particularităţile „*Oraşului inteligent*", ne permite:

- imaginarea/proiectarea domeniilor de dezvoltare a acestor comunităţi urbane;
- posibilitatea includerii proiectelor ce vizează dezvoltarea sistemelor (şi serviciilor) urbane, într-o posibilă agendă virtuală.

Oraşele inteligente. Caracteristici

Am utilizat conceptul „*Oraş Inteligent*". Fără a încerca să re/definim acest concept (varietatea tehnologiilor care au fost implementate sub această etichetă oferind, totuşi, posibilitatea exprimării unor, diverse, puncte de vedere), am indica existenţa unui tip de aşezare urbană aptă să facă faţă tuturor nevoilor cetăţenilor, instituţiilor, companiilor etc., din punct de vedere economic, social, cultural, ambiental. Astfel, un oraş poate fi numit „*inteligent*", doar, atunci când investiţiile în capitalul uman, social, în infrastructura de energie (electricitate, gaz), în comunicaţii, transport, servicii de urgenţă, construcţii, echipamente publice etc., sunt gândite pentru o dezvoltare durabila (pe termen lung) şi asigură un nivel de trai ridicat, cu o gestiune avizată şi echilibrată a resurselor naturale, toate susţinute de o administraţie performantă şi participativă.

În acest context, menţionăm şi caracteristicile/specificul „*oraşului inteligent*". Un „*oraş inteligent*" este o zonă/arie urbană care în care sunt utilizate diferite tehnici/tehnologii dedicate colectării datelor necesare gestionării eficiente a resurselor. Colectarea datelor de către municipalitatea respectivă implică (conform strategiei adoptate) terţi/privaţi, locuitorii oraşului[2] sau/şi utilizarea unor senzori electronici dedicaţi; avem în vedere datele colectate în vederea procesării şi analizării lor, pentru a monitoriza și administra, de exemplu, sistemele de trafic şi de transport, centralele electrice, reţelele de alimentare cu apă, procesarea/neutralizarea deşeurilor, aplicarea legii, diverse sisteme informatice, facilităţi şi utilităţi. Conceptul „*oraş inteligent*" integrează domenii precum tehnologia informaţiei şi comunicaţiilor

[2] Implementarea senzorilor, deţinerea şi/sau utilizarea lor se poate realiza în conformitate cu strategiile adoptate, menite să optimizeze eforturile municipalităţii, să implice agenţii economici sau/şi să responsabilizeze cetăţenii, principalii beneficiari ai investiţiilor realizate.

• În anumite situaţii senzorii urbani şi informaţiile generate sunt/au fost proprietatea unor companii private; constatăm, astfel, existenţa unui anumit nivel de condiţionare, inclusiv financiară, a municipalităţii;

• Ca alternativă, dând dovadă de iniţiativă şi inventivitate municipalităţile au aplicat tehnici precum „donarea de date„, reducând costurile de achiziţie, implementare şi mentenanţă a senzorilor urbani (ex., dezvoltarea şi distribuţia unor aplicaţii dedicate telefoanelor „inteligente", oferind cetăţenilor posibilitatea raportării datelor colectate, vezi „Street Bump" pentru raportarea drumurilor prost întreţinute).

În alte situaţii,însă, chiar dacă colectarea (de asemenea, actualizarea şi menţinerea) informaţiilor obţinute (considerate critice) este necesară, există un anumit nivel de risc dacă anumite informaţii devin publice.

Constatăm:

• contradicţia între nevoia liberului acces la informaţii şi caracterul privat al anumitor informaţii personale;

• existenţa/utilizarea unei practici de anonimizare a datelor.

(IT&C), „IIOT"[3]/ „IOT", precum și o gamă diversă a dispozitivelor fizice conectate la rețea și a soluțiilor software, dedicate optimizării eficienței operațiunilor, sistemelor urbane, *„serviciilor de oraș*". Tehnologia „*orașului inteligent*" permite oficialilor orașului/ Municipalității să interacționeze, direct, cu infrastructura comunitară (cu orașul !) și să monitorizeze ceea ce se întâmplă în oraș și modul în care orașul evoluează.

Este esențial să facem distincția între existența (și administrarea) „*orașul inteligent*" și implementarea unor proiecte – fragmentate – specifice unui „*oraș inteligent*" (atenție, lipsa concepției generale, dă naștere unor inițiative/activități costisitoare, nesustenabile!).

Poate ar fi interesant să menționăm și „*ce nu este un oraș inteligent*"!

Nu este un „*oraș inteligent*":

- cel în care municipalitatea nu a avut, măcar, o inițiativă care să vizeze: „*Guvernanța inteligentă*", „*Mediul inteligent*", „*Economia inteligentă*", „*Mobilitatea inteligentă*".
- cel în care Municipalitatea nu a încercat să abordeze rezolvarea cerințelor/ necesităților comunității pe care o deservește, utilizând soluții IT&C (în diferite forme de parteneriat, între părțile interesate: public/privat, municipalitate/locuitori);
- cel în care nu se poate identifica planificarea, operarea, dezvoltarea și administrarea unor activități specifice domeniilor: „*Domeniul Digital*"), „*Domeniul Sustenabilității*", „*Dezvoltării durabile*".

Cyberspace. Interconectarea tehnologiilor, schimbul de informații

Am prezentat ce este și ce nu este „*orașul inteligent*".

La fel de interesantă ar putea fi și prezentarea „*spațiului*", în care identificăm existența și evoluția unui „*oraș inteligent*".

În conformitate cu specificul obiectivelor urmărite în procesul de colectare, procesare și interpretare/analiză a datelor colectate „*orașul inteligent*„ poate fi poziționat/raportat la/în diverse ecosisteme precum: ecosistemul terestru/ecosisteme subiacente, sau/și „*ecosistemul cibernetic*" (cf. Department of Homeland Security – raport publicat în martie 2011, „*Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*").

Imaginând diversitatea preocupărilor, actorilor/agenților, resurselor specifice, aducem astfel în discuție existența „*ecosistemului cibernetic*", o comunitate complexă de dispozitive, rețele, oameni și organizații care interacționează, mediul și tehnologiile care susțin aceste interacțiuni.

Abilitatea „*ecosistemului cibernetic*" de a simplifica schimbul de informații este, în același timp, cel mai mare beneficiu și cea mai mare amenințare. Această dualitate aduce în discuție, inerent, vulnerabilitățile, amenințările și riscurile asociate domeniului cibernetic.

Astfel, reacționând favorabil atunci când constatăm beneficiile extinderii „*ecosistemului cibernetic*" (și necesitatea actualizării tehnologiilor în vederea

[3] „*Industrial Internet of everything", „Internet of everything".*

maximizării beneficiilor), trebuie să avem în vedere şi posibila vulnerabilizare a reţelelor/sistemelor informatice şi producere a unor blocaje ce pot declanşa, rapid, o succesiune „*în cascadă*" a evenimentelor, provocând astfel posibile dezastre tehnologice, pe scară largă, în întreaga reţea şi comunitate

Aici, trebuie să menţionăm că:

- suntem, cu toţii, subiecţi ai „*forţelor dinamice"* identificate în ecosistemele biologice, ce dictează regulile prin care entităţile vii se dezvoltă, se maturizează şi mor. În societatea contemporană, atât organizaţiile, cât şi indivizii sunt adesea expuşi, accidental/voit, la patologiile şi efectele de contagiune ce se pot dezvolta într-un ecosistem.
- prea des, securitatea cibernetică este considerată a fi, exclusiv, domeniul IT. Totuşi, apreciem că progresăm spre un viitor în care abordarea interdisciplinară va fi crucială în guvernanţa şi managementul sistemelor complexe (ex. vezi managementul riscului în sistemele complexe) precum şi în tratarea vulnerabilităţilor, fragilităţii şi defecţiunilor sistemice.

Ecosistemul cybernetic („cyberspace"), un sistem complex, intrinsec periculos

(Trebuie să ne temem ?)

Sistemele complexe, asociate dezvoltării / activării „*oraşelor inteligente*" (de exemplu, specifice asigurării/monitorizării/optimizării transportului, dedicate asistenţei medicale, generării energiei, etc.) pot fi, în mod inerent, periculoase (prin propria natură).

Riscurile relevante pot fi tratate[4] (opţiuni de tratare: evitarea riscului, reducerea riscului, înlăturarea sursei riscului, schimbarea consecinţelor, modificarea probabilităţilor, împărţirea riscului cu alţii, menţinerea nivelului riscului, sau creşterea nivelului riscului pentru a urmări o anumita oportunitate), frecvenţa expunerii la pericolele relevante poate fi uneori schimbată, însă procesele implicate în sistem sunt, intrinsec, periculoase; tocmai prezenţa acestor pericole determină crearea mecanismelor de adaptare, auto-organizare şi apărare relevante.

Magnitudinea/importanta şi specificul consecinţelor unui posibil eşec conduc, în timp, la construirea mai multor straturi de apărare (identifică astfel „*adaptarea*").

Această protecţie include:

- componente tehnice, relevante (de ex. sistemele backup, caracteristici de siguranţă ale echipamentelor);
- componentele umane (de exemplu, realizarea unor activităţi dedicate formării personalului, îmbunătăţirii cunoştinţelor şi abilităţilor relevante);
- o varietate de mecanisme de apărare implementate la nivelul organizaţiei, conform normelor de reglementare, sau bunelor practici (de exemplu, politici şi proceduri, certificare, reguli de lucru, formare în echipă).

[4] Tratarea riscului este, în fapt, un proces de modificare a riscului;implica alegerea şi implementarea uneia sau mai multor optiuni de tratare. Odata ce un tratament a fost implementat, el fie devine un control, fie modifica acele controale deja existente.

Sisteme complexe. Existenţa actorilor adaptativi, asigurarea controlului

Am menţionat, astfel, coabitarea conceptelor ce adresează „adaptarea" şi „reglementarea".

Într-un „*sistem complex*" elementele sale sunt dificil de separat. Deoarece elementele sunt interdependente, viitorul lor depinde nu numai de condiţiile iniţiale şi cele limită, ci şi de interacţiunile care au loc/au avut loc în timp şi spaţiu, generând informaţii noi.

Informaţiile generate de interacţiuni, limitează predictibilitatea. Deoarece tehnicile tradiţionale, cum ar fi „*optimizarea*", se bazează pe predictibilitate, nu pot face faţă complexităţii, din ce în ce mai mari, a sistemelor. În acest context, „*adaptarea*" şi „*auto-organizarea*" nu neapărat, „*reglementarea*" (!) pot permite/ facilita schimbarea comportamentelor, în funcţie de situaţia constatată (Gershenson, 2013a; Rauws and De Roo, 2016).

Aşa cum menţionam, adaptarea, capacitatea de a răspunde evenimentelor specifice mediului, este foarte importantă; se poate obţine (chiar) şi „*autoorganizare*" fără „*adaptare*", însă „*adaptarea*" este acceleratorul major.

Exemplu. Lipsa, sau/şi insuficienţa capacităţii de adaptare a tehnologiilor „învechite" determina necesitatea proiectării şi implementării acestora, „*de sus în jos*" (totul era predefinit, predeterminat).

În timp, dezvoltarea şi utilizarea dispozitivelor de comunicare, a protocoalele partajate dedicate, au facilitat nu doar sincronizarea stărilor, însă, chiar şi posibila stare de „*auto-organizare*". Prin intermediul interacţiunilor neliniare, agenţii din sistem îşi pot sincroniza stările şi îşi pot coordona activităţile. În mod obişnuit, sunt necesare protocoale şi platforme interoperabile (de exemplu, în cazul „*oraşelor inteligente*" sunt utilizate platforme ce permit diferitelor dispozitive să comunice/ transfere informaţii şi să se coordoneze: prin stratificarea unei reţele de telecomunicaţii conexată reţelei de electricitate, producătorii şi consumatorii se pot adapta şi se pot organiza, în scopul optimizării, controlării echilibrului de sarcină, în sistem). Interacţiunea – densă, neliniară, în reţea – este un element-cheie în promovarea apariţiei unui model (global) de organizare.

În acest context, putem defini „*adaptarea*" şi ca o schimbare la nivel „*agent*" sau/şi „*sistem*", răspuns la o stare a mediului ce va ajuta „*agentul*" sau/şi „*sistemul*" să-şi atingă obiectivele (Gershenson, 2007).

Studiul „*adaptivităţii*" în cadrul sistemelor, a început cu decenii în urmă, ştiinţa numindu-se „*Cibernetica*" (în Cibernetică, relevanţa demersurilor ştiinţifice vizează şi încercarea studierii fenomenelor, independent de substratul lor, primând importanţa funcţiei sistemelor, nu compoziţia acestora).Obiectul de studiu al Ciberneticii actuale, este „*Sistemul Adaptiv Complex*".

Un „*Sistem Adaptiv Complex*" („*CAS*") este compus din „*agenţi*" individuali, care au libertatea de a acţiona în moduri ce nu sunt total predictibile şi ale căror acţiuni sunt interconectate, astfel încât acţiunile unui agent schimbă contextul pentru alţi agenţi.

De ce am fi tentaţi să menţionăm aceste sisteme într-o prezentare ce relaţionează "*ecosisteme tehnologice*", „*oraşe inteligente*" şi „*infrastructuri critice*" ?

Un posibil răspuns ar avea în vedere modul în care componentele sistemului se adaptează sau (se) învaţă pe măsură ce interacţionează, Sistemele Adaptive

Complexe, aflându-se în centrul unor probleme contemporane importante (studiul CAS prezintă provocări unice, utilizarea unora dintre cele mai puternice instrumente matematice oferind un ajutor limitat !).

Într-un „*Sistem Adaptiv Complex*", comportamentul agenţilor este, în mod obişnuit, guvernat de reguli destul de simple, care duc la apariţia unor modele „*auto-organizat*e" de comportament.

Auto-organizarea poate fi identificată în crearea spontană a unui model coerent, rezultat în urma interacţiunilor, locale, dintre componentele, iniţial, independente.

Pot exista, în esenţă, doua moduri în care se poate asigura/realiza coordonarea necesară funcţionarii, la nivelul unui sistem:

1) Prin implementarea unor reguli impuse sistemului, ca urmare unor influenţe externe. Avem în vedere, exclusiv, activităţi de reglementare, nu şi intervenţia la nivelul proceselor.

2) Prin configurarea sistemului, în urma interacţiunii diferitelor sale componente. În cadrul sistemelor complexe ce au potenţialul de a activa un "*oraş inteligent*", (ex. reţele inteligente de energie electrică, reţele de transport sau reţele logistice) elementele deţin o anumita formă de autonomie, necesară alegerii căilor de acţiune.

Din acest motiv, aceste sisteme nu sunt produsul metodelor tradiţionale de design „*de sus în jos*" (structura generală a sistemului este un produs al interacţiunilor, locale, între componente).

Există o serie de premise esenţiale, care trebuie să fie prezente, pentru ca acest proces de auto-organizare să se poată realiza.

- Trebuie să existe componente/caracteristici aleatorii în starea iniţială a sistemului, variaţii între stările componentelor, elemente cu diferite nivele de autonomie şi conexiuni neliniare locale (nu există posibilitatea auto-organizării atunci când sistemul este deja proiectat şi deţinut/administrat într-o structură bine definită şi ordonată).

Exemplu: într-o abordare de tipul „*de sus în jos*", asociind sistematizării, concepte precum „*reglementarea*" şi „*centralizarea*", într-un oraş sunt prevăzute (în anumite zone, predeterminate) facilităţi dedicate desfăşurării anumitor procese. Cetăţenii şi agenţii economici se vor organiza în consecinţă.

Însă, dacă există zone „*nereglementate*", în jurul oraşului (de exemplu), se poate ajunge la o stare de auto-organizare nedorită. Lipsa controlului centralizat şi existenţa actorilor adaptativi (care interacţionează), generează o anumită formă de apariţie – spontană – a ordinii.

- De asemenea, componentele sistemului trebuie să fie eterogene. Heterogenitatea este importantă (dacă toate componentele au deja aceeaşi stare, atunci ele sunt sincronizate şi nu este nevoie de auto-organizare).

Asigurarea rezilienţei

În diferite lucrări/articole adresând „*securitatea distribuită*", se recunoaşte necesitatea funcţionării dispozitivelor cibernetice, împreună, (aproape) în timp real, pentru a minimiza frecvenţa şi magnitudinea atacurilor cibernetice şi a asigura

apărarea împotriva lor. Aceasta este o formă a monitorizării continue, în care participanţii relevanţi („*agenţii*") interacţionează pentru a asigura securitatea şi menţinerea unei stări de siguranţă persistentă (similar sistemelor biologice, identificăm coexistenţa multor „*agenţi*", printre care dezvoltatori de sisteme/ analişti de securitate, utilizatori/ manageri şi hackeri, care interacţionează pentru a produce un mediu dinamic şi în continuă evoluţie, în care comportamentul este emergent.

Astfel, cu uşurinţă putem afirmă că acest/un context, în care se gestionează informaţii şi activităţi relevante asigurării securităţii cibernetice, poate fi abordat şi ca un „*Sistem Adaptiv Complex*" (CAS). În contextul menţionat, identificăm (şi) existenţa ofertei „*comunităţii tehnice*", constând în garanţii şi proceduri relevante sistemelor dedicate asigurării securităţii, de obicei, furnizate de către sectorul privat. Într-un astfel de sistem, design-ul şi adecvarea controalelor – implementate – facilitează schimbul de informaţii, interacţiuni şi comportamente, obţinându-se rezultate benefice.

Pe măsură ce sistemele de securitate devin mai complexe, entităţile relevante asigurării securităţii sunt nevoite să se adapteze pentru a-şi optimiza comportamentul – proces denumit „*evoluţie*".

Astfel, apar diferite forme de organizare, sistemul manifestând comportamentul inteligent în baza schimbului de informaţii şi a unor proprietăţi precum: „*emergenţa*", „*co-evoluţia*", „*varietatea necesară*", „*conectivitatea*", „*auto-organizarea*" şi „*instabilitatea*".

Controlul „*CAS*" tinde să fie/devină foarte dispersat şi descentralizat. Un comportament coerent poate să fie prezent/activ în sistem; acest comportament provine din competiţia şi/sau cooperarea dintre agenţii înşişi. Comportamentul general al sistemului este rezultatul numeroaselor decizii, luate în fiecare moment, de mulţi agenţi individuali. Astfel, vizăm caracteristicile esenţiale ale „*Sistemelor Adaptive Complexe (CAS)*", precum „*Auto-organizarea*"(ordinea spontană care apare atunci când sistemul trece la un nou mod de organizare pentru a răspunde la influenţele exercitate de mediul înconjurător), „*Emergenţa*" (tranziţia de la regulile locale către principiile globale, sau stările generale care însoţesc mulţimea agenţilor) şi crearea unei „*noi ordini*".

Într-un context, caracterizat prin dinamica formelor de organizare, accelerarea diversificării infrastructurii şi volumul mare al informaţiilor tranzacţionate (constatate şi la nivelul infrastructurii „oraşului inteligent"), având în vedere atât ameninţările potenţial catastrofale – o realitate în mediul cibernetic- cât şi necesitatea remodelării mediilor dedicate operaţiunilor cibernetice în scopul creşterii siguranţei şi sustenabilităţii operaţiunilor specifice/relevante, aducem în discuţie posibilitatea vulnerabilizării reţelelor/sistemelor, adresând (şi) cerinţa asigurării „*rezilienţei*": abilitatea de „a rezista, a reacţiona şi a se reface".

Organizaţiile din categoria „*Cyber-resilient*" nu se bazează doar pe implementarea soluţiilor tehnologice tradiţionale (exemplu „*firewall*") sau/şi a proceselor dedicate (cum ar fi administrarea controlului accesului) actualizându-şi abordarea, asociind rezilienţei, cultura organizaţională, leadership-ul şi strategiile dedicate managementului

şi securizării reţelelor, creându-şi astfel, un avantaj durabil în raport cu alte organizaţii şi/sau criminalitatea cibernetica.

Concluzie

În contextul indicat de existenţa şi particularităţile unui „*oraş inteligent*", indiferent dacă vorbim despre Internet, o reţea inteligentă de energie electrică, reţele de transport sau reţele logistice, (în aceste sisteme complexe) elementele deţin/trebuie să deţină o anumită formă de autonomie, necesară alegerii căilor de acţiune (structura generală a sistemului este un produs al interacţiunilor, locale, între componente.

Ecosistemul cibernetic, tehnologiile ce activează „*oraşele inteligente*" evoluează; asigurarea rezilienţei nu a fost/nu este, deocamdată, un obiectiv îndeplinit.

Într-un mediu în care se constată anumite tendinţe – relevante, chiar şi evoluţiei ameninţărilor – abordările tradiţionale privind reglementarea, adaptarea, şi auto-organizarea, vor fi văzute, din ce în ce mai mult, ca fiind „*necesare, dar nu suficiente*".

Un ecosistem cibernetic, elastic, este un obiectiv valoros ce poate oferi organizaţiilor care operează în acest domeniu o încredere sporită în securitatea sistemelor şi a datelor.

Bibliografie

„Achieving resilience in the cyber ecosystem" (2014), EYGM Limited.

„What is Not a Smart City", Dr. Azamat Abdoullaev, EIS Encyclopedic Intelligent Systems Ltd

Adaptive Cities: A Cybernetic Perspective on Urban System- Rauws, W. and De Roo, G. (2016). Adaptive planning: Generating conditions for urban adaptability. lessons from dutch organic development strategies.

Adaptive Cities: A Cybernetic Perspective on Urban Systems- Gershenson, C.(2007). Design and Control of Self-organizing Systems.

Adaptive Cities: A Cybernetic Perspective on Urban Systems-Gershenson, C.(2013a). Facing complexity:

Cibernetica sistemelor economice, Emil Scarlat, Nora Chiriţă.

Complex-systems.com. Retrieved 6 July 2017, from http://www.complex-systems.com/pdf/16-1-2.pdf

Corneliu Rusu (2000), Management strategic, Bucureşti, Editura ALL Back.

Environment and Planning B: Planning and Design.

Fuchs.uti.at. Retrieved 6 July 2017, from http://fuchs.uti.at/wp-content/uploads/selforganization.pdf

Gabriela Sabău (2001), Societatea cunoaşterii, o perspectivă românească, Bucureşti, Editura Economică.

How Complex Systems Fail

http://web.mit.edu/2.75/resources/random/How%20Complex%20Systems%20Fail.pdf
Policies /Policy Department A:Economic and Scientific Policy („This report was commissioned to provide background information and advice on Smart Cities in the European Union -EU- and to explain how existing mechanisms perform")
Prediction vs. adaptation. In Complexity Perspectives on Language, Communication and Society, A. Massip and A. Bastardas, (Eds.). Springer, Berlin Heidelberg.
Self-Organizing Networks. Ericsson.com. Retrieved 6 July 2017, from https://www.ericsson.com/en/publications/books/self-organizing-networks
Studiu: „Mapping Smart Cities in the EU" (2014)/European Parliament/Directorate General for Internal